RAPID DELIVERY OF CYBER CAPABILITIES: EVALUATION OF THE REQUIREMENT FOR A RAPID CYBER ACQUISITION PROCESS

GRADUATE RESEARCH PROJECT

Matt J. Butler, Major, USAF

AFIT/ICW/ENG/12-03

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

The views expressed in this report are those of the author and do not reflect the official policy or position of the United States Air Force, the Department of Defense, or the United States Government. This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

AFIT/ICW/ENG/12-03

RAPID DELIVERY OF CYBER CAPABILITIES: EVALUATION OF THE REQUIREMENT FOR A RAPID CYBER ACQUISITION PROCESS

GRADUATE RESEARCH PROJECT

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Cyber Warfare

Matt J. Butler, BS, MA

Major, USAF

June 2012

AFIT/ICW/ENG/12-03

RAPID DELIVERY OF CYBER CAPABILITIES: EVALUATION OF THE REQUIREMENT FOR A RAPID CYBER ACQUISITION PROCESS

Matt J. Butler, BS, MA

Major, USAF

Approved:

Jonathan W. Butts, PhD (Chairman)

30 May 2012
Date

Robert F. Mills, PhD (Member)

30MAY/12
Date

AFIT/ICW/ENG/12-03

Abstract

The Department of Defense has a standardized acquisition construct for delivering capabilities in the land, air, sea and space domains. Recently, cyberspace was identified as a warfighting domain; however, the unique attributes of the cyberspace domain require a more rapid process to deliver capabilities to the warfighter. Indeed, from initial requirements to fielding of the F/A-22 aircraft was approximately 20 years; this timeframe is not acceptable for cyberspace capabilities.

To address requirements associated with the quickly evolving technology, senior leaders have called for a rapid cyber acquisition strategy. In response, methodologies have been proposed to enable quick response acquisition programs. On the surface, this notion appears viable. Examination, however, reveals that there has yet to be an Air Force program within the cyberspace domain that necessitates a rapid acquisition process. Rather, findings demonstrate that requirement for rapid delivery of cyberspace capabilities is more aptly associated with fielding tactics, techniques and procedures (TTP). This research examines the rapid delivery of cyberspace capabilities and challenges the paradigm associated with the need for rapid cyber acquisition. Results of the research demonstrate a need to shift focus from rapid acquisition to rapid TTP delivery.

Acknowledgments

First off, I would like to thank my research advisors for providing the guidance and feedback on conducting research on a realm that is in a continual state of flux. There is still so much to discuss when it comes to cyber acquisition. This research was only a small pebble to the road that still lies ahead of us.

I would also like to thank my classmates for helping educate me on the new domain that is having world changing impacts on us. I felt a little overwhelmed at times being somewhat of an outsider to the world of cyberspace but you have all embraced that and helped develop me to become a more educated officer for today and tomorrows cyberspace challenges.

In addition, I owe a huge debt of gratitude to my wife who supported and endured my undecipherable ramblings on my graduate research project. Her encouragement and constant support were integral to the research and without it I would still be staring at the first page.

Lastly, I want to thank my mom for her continual encouragement that has gotten me to where I am today.

Matt J. Butler

Table of Contents

Page

List of Figures

List of Tables

Table Page

List of Abbreviations

ACC – Air Combat Command

AFI – Air Force Instruction

AFNet – Air Force Network

AFSPC – Air Force Space Command

AOC – Air and Space Operations Center

CCS – Cyber Control Station

CWG – Cyber Working Group

AF DCGS – Air Force Distributed Common Ground Station

DCO – Defensive Cyber Operations

DGO – Department of Defense Global Information Grid Operations

FYDP – Future Year Defense Program

GIG – Global Information Grid

IOP – Information Operations Platform

MS – Milestone

NCCT – Network Centric Collaborative Targeting

NDAA – National Defense Authorization Act

OCO – Offensive Cyber Operations

PE – Program Element

POM – Program Objective Memorandum

PoR – Program of Record

RIC – Resource Identification Code

RTO&I - Real Time Operations and Innovation

TTP – Tactics, Techniques and Procedures

VLMS – Vulnerability Life Cycle Management

WS – Weapon System

THE STATE OF CYBER ACQUISTIONS

I. Introduction

"The one guarantee in today's cyberspace domain is that it will be different in the future. In the physical domains, the laws of nature never change. We can count on gravity as a constant. In the cyberspace domain, the rules of humans dominate and we can't count of that stability" [27].

Lieutenant General Michael J. Basla
Vice Commander of Air Force Space Command

Top United States (U.S.) civilian and military leaders understand that the same classic acquisition strategy used to acquire one of the Air Force's (AF) newest fielded fighter aircraft, the F/A-22 Raptor, is not sufficient going forward. From the date of its initial requirements to fielding, was approximately 20 years. From a cyber perspective, the software onboard the F/A-22 was developed back in 1983 by International Business Machines [30]. With that said, it is fairly intuitive that the acquisition used for the F/A-22 will not work for the network speed evolving technology that is driven by such things as Moore's law. Moore's law states the microprocessor processing power doubles about every 18 months [5]. Another way to view Moore's Law is it is a prediction of technological progress and explains why the computer industry has been able consistently to produce products that are smaller, more powerful and less expensive than their predecessors [5]. Indeed, the cyberspace domain cannot be treated as acquisition equals to the air and space domain.

Cyber acquisition is a major challenge for the Department of Defense (DoD) and many attempt to compare analogies to other domains. This is not the first time this predicament has surfaced. The scenario played out over 30 years ago with the establishment of Air Force Space Command (AFSPC). General William Shelton, the commander of AFSPC, stated at a recent Armed Forces Communications and Electronics Association conference that "some of the challenges include establishing some much needed lanes in the road, adjusting the acquisitions process to reflect the nature of cyber products, and expediting a fundamental culture shift across the AF from cyberspace support mindset to one of cyberspace operations" [12].

One reason cyberspace is such a challenge is an inherent lack of flexibility in the rigid construct that has been in place for many years - a construct that works quite well for the air and space domain. Figure 1 profiles a graphical depiction of the rigid construct for acquisitions, called the Integrated Defense Acquisition, Technology, and Logistics (AT&L) Life Cycle Management System. Understandably, this chart is difficult to understand and comprehend; however, it helps demonstrate that the traditional, or what some Defense Acquisition University (DAU) certified professionals term “big acquisitions”, is very lengthy and rigid.

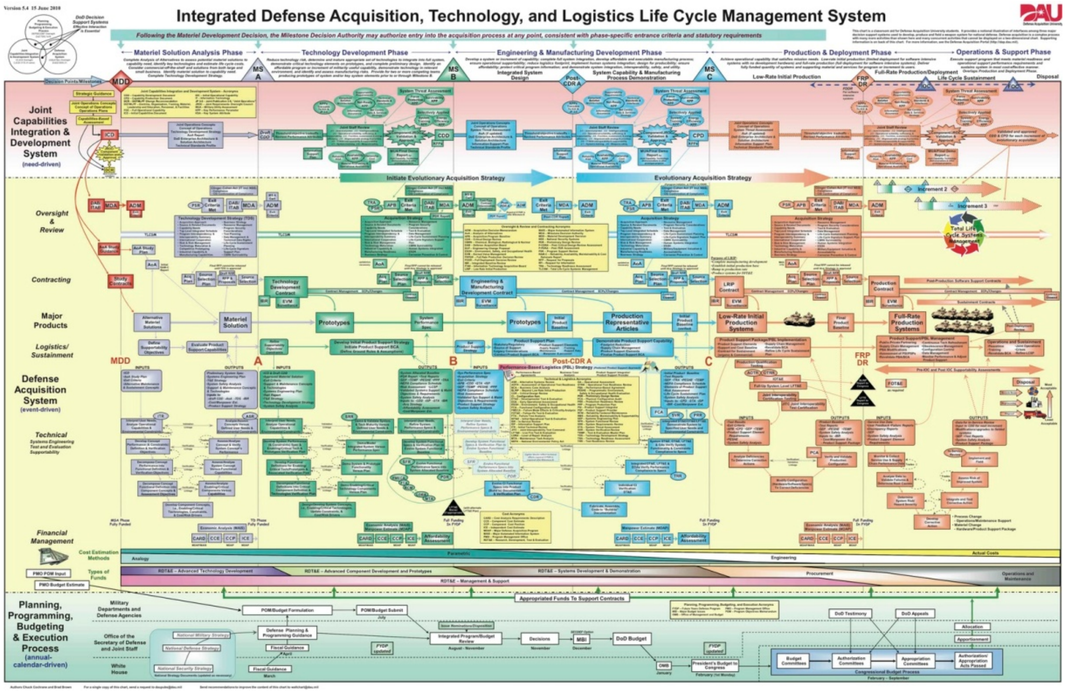

Integrated Defense Acquisition, Technology, and Logistics Life Cycle Management System
Version 5.4 15 June 2010
DAU
Materiel Solution Analysis Phase
Technology Development Phase
Engineering & Manufacturing Development Phase
Production & Deployment Phase
Operations & Support Phase
MDD
MS A
MS B
MS C
Post-CDR A
FRP DR
Joint Capabilities Integration & Development System (need-driven)
Oversight & Review
Contracting
Major Products
Logistics/ Sustainment
Defense Acquisition System (event-driven)
Technical
Financial Management
Initiate Evolutionary Acquisition Strategy
Evolutionary Acquisition Strategy
Prototypes
Planning, Programming, Budgeting & Execution Process (annual-calendar-driven)
Military Departments and Defense Agencies
Office of the Secretary of Defense and Joint Staff
White House

Figure 1 Integrated Defense AT&L Life Cycle Management System

Cyberspace has evolved to the point that the AF is treating it as an additional war-fighting domain, alongside air and space. Cyberspace is the global domain within the information environment consisting of the interdependent network of information technology (IT) infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers [4]. Indeed, cyberspace is the domain where cyber operations are conducted. Cyber operations are the employment of cyber capabilities within the cyberspace domain. An example cyber operation is computer network activities to operate and defend within the Global Information Grid (GIG) [4]. Note that the terms cyber operations and cyberspace operations are interchangeable and, for the purposes of this research, considered synonymous.

One of the unique attributes of cyberspace is that it is a man-made domain, and is therefore unlike the natural domains of air, space, land, and maritime. It also requires continued attention from humans to persist and encompass the features of specificity, global scope, and emphasis on the electromagnetic spectrum. Cyberspace nodes physically reside in all domains. Activities in cyberspace can enable freedom of action for activities in the other domains, and activities in the other domains can create effects in and through cyberspace [4]. The cyberspace domain is now a primary conduit for transactions vital to every facet of modern life. Society and military are increasingly dependent on cyberspace. Indeed, cyberspace is a source of strength and a potential vulnerability to national security. While cyberspace operations enable a modern society, they also create critical vulnerabilities for adversaries to attack or exploit.

These potential national security vulnerabilities have not arisen overnight; the AF has been engaged in cyber initiatives for quite some time. For example, the AF has been committed to developing new offensive and defensive capabilities to support network operations since the mid-1990s. In 2003, cyberspace was described as the nerve network of the defensive infrastructure for the industrial control system of the country [6]. Cyberspace compromises hundreds of millions of interconnected computers, servers, routers, switches, fiber optic cables, and wireless devices that make the critical infrastructure function. Also, the boundaries of cyberspace are not confined to the tangible IT components which enable technological capability.

Lieutenant General William Lord, the AF’s chief information officer (CIO), summarized dependence on cyberspace in a quote to the Air Force Association that "the network is now so integral to combat operations that you can't live without it," and went on to say "twenty years ago, when the network went down, who cared?” [37]. It is no longer an option to unplug from cyberspace reliance and there needs to be a viable acquisition and testing process in place that can adapt to the speed of IT advancements.

Currently, the first step to attaining a new cyber capability within the AF is to put it through the traditional acquisition construct, which acquire quality products that satisfy the user’s needs with measurable improvements to mission capability and operational support, in a timely manner, and at a fair and reasonable price [3]. DoD policy dictates the defense acquisition system be flexible, responsive, innovative, disciplined, streamlined, and have effective management. The cyber community argues the responsiveness for cyberspace is a concern for new and emerging IT; especially considering Moore's law. Recently, General William Shelton, commander of AFSPC, spoke out at recent conference in a "soapbox rant" about the military's approach to acquiring cyber capabilities. General Shelton, who oversees AF and cyberspace operations, said the DoD "acquires cyber capabilities the same way it buys aircraft or satellites – a process that can take years, while new developments in computer hardware and software can happen in days or months". He went on to say he is "frustrated by the lack of speed," in cyber acquisitions [18].

1.1 Problem Statement

The military leaders of today believe there needs to be a rapid cyber acquisitions approach. However, is this claim substantiated based on current operations and requirements? This research seeks to answer the following question:

- Is there a need for a rapid cyber acquisition approach in the Air Force?

The following questions will provide indications to help determine the overall finding:

- What is the current cyber acquisition paradigm?
- Is the current paradigm sufficient or insufficient for rapid cyber acquisition?
- What is the optimal method for delivering rapid cyber capabilities?

1.2 Research Focus

This research examines the current laws for the traditional acquisition approach and determines if there should be a separate process for rapid cyber acquisitions. Specifically, the research explores past, current and projected cyberspace programs of record (PoR) to give both a quantitative and qualitative perspective on the rapid cyber acquisitions framework. It also investigates if cyber operations are as time sensitive as most are led to believe. Finally, the research investigates if the traditional AF testing process is unable to adapt. In other words, is there a need to acquire cyberspace capabilities as fast as what is currently briefed by military leadership today.

There is an apparent inconsistency in the use of the term PoR. Many people use the term PoR to indicate initiatives or developments that have come to fruition from resources or organizations. For example, an internal database for tracking data developed within a squadron is not a PoR. However, a PoR is a program that has prevailed the program objective memorandum (POM) process and is listed as a future year defense program (FYDP). The two main elements of a FYDP are the program element (PE) and resource identification code (RIC). The PE is the smallest resource aggregation controlled by Office of the Secretary of Defense (OSD). Over the course of a PoR's lifecycle it will typically use several PEs. Currently, the cyber acquisition community is trying to find the best way to translate programs onto the FYDP, for example, using a PE for defensive versus offensive programs.

1.3 Scope

Cyber acquisition is a complex topic that does not yet have a solidified framework. To scope this research, a comprehensive review of past, present and planned cyber PoR and other initiatives that could become future PoRs is performed. Requirements development, research and development (R&D) and funding are just as important discussion topics to cyber acquisitions; however, to keep the paper scoped they are only lightly discussed.

The researched cyber PoRs are categorized under the categories of offensive cyber operations (OCO), defensive cyber operations (DCO) and Department of Defense Global Information Grid operations (DGO). These categories are outlined in the "DoD Strategy for Operating in Cyberspace" [37]. There are many PoRs within the AF that are cyber support programs; for example, the air and space operations center weapon system (AOC WS) or the Air Force distributed common ground station (AF DCGS) enterprise. Both of those PoRs consist of numerous software and hardware systems that are networked together with IT but are not considered within one of the three categories described above.

The research contained in this paper is unclassified. The report also does not include material that is considered a special access program or special access required material. Although programs in the classified realm may exist, it is expected the underlying premise and conclusion are still applicable.

1.4 Approach

The theory from top U.S. civilian and military leaders is there needs to be a rapid approach to obtaining and deploying cyber capabilities. The term "rapid" is used throughout the paper and implies faster than the traditional acquisitions process. The term rapid can also be visualized in the three tiered graphic in Figure 2 which describes it as “weeks to months.”

The examination phase of the research report examines the past, present, and planned cyber PoRs. Various organizations were contacted within AFSPC, Air Force Operational Test Center (AFOTEC), Air Combat Command (ACC), Air Forces Cyber (AFCYBER) and other agencies within the DoD to obtain their thoughts and theories, and other relevant material to rapid cyber acquisitions. The second phase of examination was to determine what unclassified documentation is available. The unclassified documentation reviewed included test plans, test reports, test priority lists, DoD/AF Instructions, memorandums, conference briefings, prior research, and miscellaneous material that provide insight into the rapid cyber acquisitions workings. The offices contacted for this research are listed in the back of this document in Appendix C.

1.5 Organization

The remaining research is organized as follows: Chapter 2 examines the changes associated within the AF cyber community in the past couple years. Chapter 3 discusses the acquisitions process. Chapter 4 provides a discussion of tactics, techniques and procedures (TTP) within the cyber environment. Chapter 5 provides analysis and discussion, and Chapter 6 provides conclusions and recommendations.

II. Background

"US Cyber Command has been in existence for more than a year, and no one familiar with the command or its mission believes our current policy, law or doctrine is adequate to our needs or our capabilities"[26].

General Michael V. Hayden, USAF, Retired
Former Director, National Security Agency
Former Director, Central Intelligence Agency

The cyber realm within the AF has been in a state of flux since the initial stand up of Twenty-Fourth Air Force (24 AF); which is also known as AFCYBER. This chapter discusses what has transpired within the cyber community to augment a rapid acquisitions approach to the cyber domain. Note that the terms within the cyber realm have also been fluxuating constantly as well. For example, over the past few years the term has morphed from "agile" to "rapid" to "responsive" cyber acquisitions. The end result is to provide a cyber capability to the end-user in a faster fashion and to ensure it is not hindered by the traditional acquisition approach.

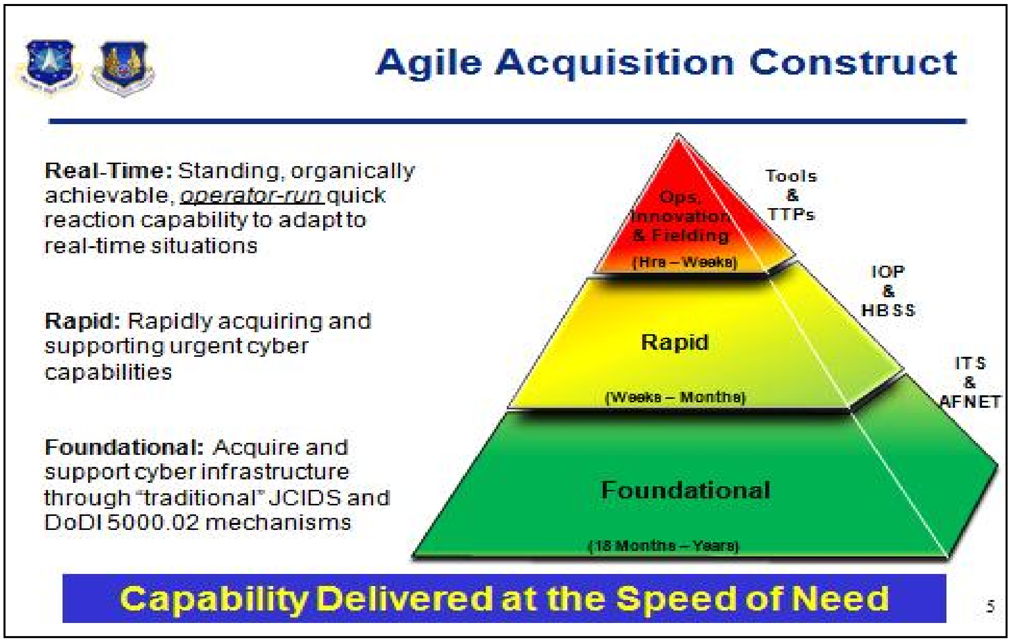
2.1 AFCYBER

The establishment of AFCYBER was proposed as a Major Command (MAJCOM) to exist in a provisional status until the construct could be finalized. In October of 2008 the AF announced that AFCYBER was not going to be activated as its own MAJCOM, but rather would transition into 24 AF within AFSPC. The original purpose of AFCYBER was to develop a MAJCOM that could stand alongside AFSPC and ACC as the provider for forces that the U.S. President, combatant commanders and the American people can rely on for preserving the freedom of access and commerce, in air, space and now cyberspace [12]. U.S. Cyber Command (USCYBERCOM), which stood up nearly two years ago and is a sub-unified command subordinate to U.S. Strategic Command (USSTRATCOM), is also in its infancy stage [13].

2.2 Cyber Working Group

There have been many trials and tribulations to solidifying a cyber acquisitions structure. In a 2008 Combat Air Forces conference, a cyber working group (CWG) was created that would examine alternatives for “agile” acquisition and sustainment for cyber operations. The CWG consisted of combat support agencies such as the National Security Agency (NSA), Defense Information Services Agency, DoD/AF acquisition organizations, AFSPC, USSTRATCOM, and USCYBERCOM subject matter experts (SME). The authority to stand up the CWG came from General Robert Kehler, AFSPC commander and General Donald Hoffman, Air Force Material Command (AFMC) commander. The initial CWG proposed that meeting the “speed of need” of the war fighter in the cyber domain could be accomplished through the three-tiered approach in Figure 2 which consists of operations/innovations, rapid and foundational. The approach was approved at the Corona conference in February of 2010 [2]. The CWG had some additional outside help from a leading cyber defense industry corporation to help structure the organization methodology for getting a program to the war fighter at the “speed of need.” The corporation advised a methodology to dissect the problem and helped map out a process on how to create a solution for each of the areas. Some of those focus areas were requirements, R&D, testing, and funding.

While this transformation was arising, Brigadier General James Haywood, Director of Requirements for AFSPC, directed his guidance via memorandum titled “Real Time Operations and Innovation” which laid the foundation on how a systems program office would integrate into the rapid cyber acquisitions construct [42].



Agile Acquisition Construct

Real-Time: Standing, organically achievable, *operator-run* quick reaction capability to adapt to real-time situations

Rapid: Rapidly acquiring and supporting urgent cyber capabilities

Foundational: Acquire and support cyber infrastructure through "traditional" JCIDS and DoDI 5000.02 mechanisms

Capability Delivered at the Speed of Need

5

Figure 2 Agile Acquisition Construct [39]

The three-tiered approach in Figure 2 is called the Agile Acquisition Construct and augments the identification of response to the warfighter's requirements under varying time urgent constraints [39]. The agile acquisition construct is also known as the "triage" process because it delineates the new acquisition program under one of the three tiers. By having a project fall within a tier it ensures appropriate definition of the requirements, dedication of personnel, and funding support to produce the needed capabilities within the expected timeframe. Due to the dynamic nature of the threats and the overall cyber environment, it was expected that numerous individual requirements would be identified separately on a recurring basis over a period of time, with different degrees of urgency and complexity. One method for augmenting the identification of a cyber requirement is the use of the cyber needs form (CNF) that is shown in Appendix A. The CNF is unique to the cyber acquisitions community.

Below is a description of each of the three tiers shown in Figure 2:

- Tier 3 (Foundational) – PoR that follow the joint capabilities integration and development system (JCIDS) and DoDI 5000 series processes which is discussed in the next chapter. The timeline associated with this tier is years from requirements definition to final delivery of the capability. An example PoR would be the AF network (AFNet).

- Tier 2 (Rapid) – This tier is for rapidly acquiring capabilities that are needed within the timeframe of weeks to months. The example that was relayed in Figure 2 is information operations platform (IOP) and host based security system (HBSS).
- Tier 1 (Ops, Innovations & Fielding) – This tier is for 24 AF organic means to produce capabilities needed within hours to weeks. An example of tier 1 is tactics, techniques and procedures (TTP) which is discussed in more detail in Chapter 3.

It is important to note the proposed tiers are only a notional starting point for discussion; the agile acquisition construct has not been incorporated into any AF instructions.

2.3 Big Safari

In 2010, the CWG explored another possible solution to address the ongoing issues of agile cyber acquisition. That possible solution came when senior leaders started looking to replicate an organization that had been around since the 1950s rapidly fielding high visibility programs. The 645 Aeronautical System Group (AESG), also known as the Big Safari program office, is located within the Aeronautical Systems Center at Wright-Patterson Air Force Base (AFB) in Dayton, Ohio. The Big Safari organization is well known for its expeditious fielding and weaponizing of the MQ-1 Predator/MQ-9 Reaper family of remote piloted aircraft (RPA) [2]. The office has also managed the quick turnarounds in the fielding of other well-known aircraft such as the U-2 Dragon Lady, RC-135 Rivet Joint, EC-130 Compass Call and the latest MC-12 Liberty aircraft. They also have a handful of cyber support programs within their organization such as Network Centric Collaborative Targeting (NCCT) and Project Suter.

The NCCT program is a real-time and scalable “data fusion” repository that monitors, analyzes, responds and reports on all platforms and assets that have the software/hardware installed (e.g., reconnaissance/surveillance aircraft, RPA, space and ground systems).

The other cyber support program within their inventory called, Project Suter, was named after Colonial Richard “Moody” Suter, a historic fighter pilot and initial architect of the combat exercise that is conducted yearly at Nellis AFB, Nevada called Red Flag. The Project Suter cyberspace program provides a centralized facility to integrate global electronic attack effects as part of a global operations plan. The cyber support program was also designed to deny the adversaries’ freedom of action within their own cyberspace networks. This program became the first initiative delivered to meet the specific mission requirements of AFCYBER [5].

2.4 Cyber Safari

The rapid acquisition and fielding process has worked for many years and Big Safari is already working cyberspace support programs. As such, the structure was replicated to incorporate a cyber variant called "Cyber Safari" [2].

The Big Safari program office has been successful primarily because they receive taskings directly from the Secretary of the Air Force for Acquisitions (SAF/AQ) and interface with other top level agencies and offices. The day-to-day oversight is also managed by SAF/AQ per the agreement laid out in the program management directive and letter of direction. Big Safari is not a typical program office and appeared to fit the mold for a rapid acquisition state that is needed for future cyberspace programs. Big Safari has placed cyberspace programs under different divisions within the 645th AESG because they have different acquisitions procurement process for aircraft versus the cyberspace support programs.

In 2011, the Cyber Safari office transitioned its name to XR3, which still had the same mission directive of accomplishing the following for cyber programs:

- Integration planning and deconfliction
- Program sustainment
- Planning and transition
- Rapid acquisitions support

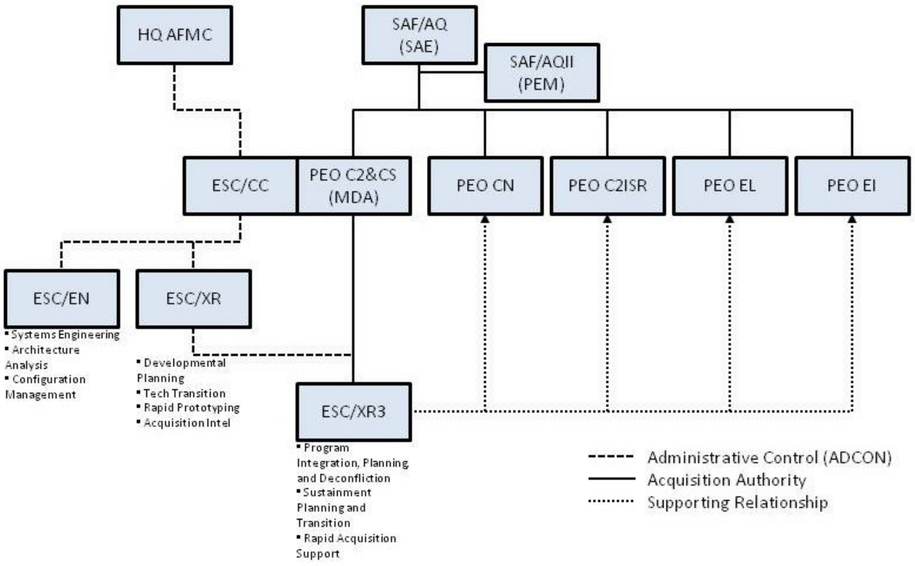


Figure 3 Rapid Cyber Acquisition Organization

Currently, the rapid acquisition organization resides administratively within Electronic Systems Center (ESC) XR organization, but operationally reports directly to the program executive officer (PEO) of command and control and combat support (C2&CS). This allows preferred staffing and the ability to reach across the ESC functional staff for support, as well as a stronger working relationship with the PEOs and their PoR organizations (see Figure 3).

2.5 National Defense Authorization Act

The organizations discussed above have helped develop the backbone construct, which was later integrated to answer Section 933 of the Ike Skelton National Defense Authorization Act (NDAA) for fiscal year (FY) 2011[1]. Section 933 of the NDAA directs the DoD to provide a strategy for the rapid acquisition of tools, applications, and other capabilities for cyberspace operations for the components of the military departments. In response, the Undersecretary of Defense (USD) for AT&L is working with the DoD cyberspace community to develop a common framework for Services and Agencies to acquire capabilities for cyberspace [34]. From this point on, the construct is referred to as NDAA rather than Section 933 of the 2011 NDAA.

This new NDAA framework supports the recently published document called “DoD Strategy for Operating in Cyberspace” and leverages related strategic cyber research and development plans [38]. The NDAA framework will provide a structure to acquire cyber capabilities across the three phases of requirements, acquisition, and testing, but also provides a new governance board. It has not yet been approved, but the governing board is planned to be set at the highest levels of the DoD, including commander of the USCYBERCOM, AF’s CIO, NSA leadership and others having missions that rely on these new rules and regulations.

2.6 Cyber Vision 2025

In April 2012, the AF started a study that was commissioned by the Chief of Staff of the Air Force (CSAF) and Secretary of the Air Force (SECAF) called Cyber Vision 2025 (CV2025). The CV2025 is being led by the AF Chief Scientist and the results are due out mid-July 2012. One of the six mission panels is investigating interests in the near/mid/far term for training, testing, and acquisitions. CV2025 shows evidence that there is a strong need and desire for structure and guidance within the cyber community as a whole.

2.7 Summary

A lot has transpired over the past few years since the construct of AFCYBER and much continues today. This chapter examined the foundations for rapid cyber development. Note that the continual flux in rules, regulation, and organizations has been encountered before within the other domains.

III. Acquisitions

"One of the biggest challenges for acquisition officials working in the cyber area is how to deliver systems at the "speed of need" [2].

Brigadier General James Haywood
Director of Requirements, Air Force Space Command

This chapter discusses the acquisition model from a high level approach and explains the most pertinent AF Instructions (AFI) relating to acquisition. The chapter also discusses testing and the AF organizations that are assigned the mission of cyber testing.

3.1 Acquisition Model

Cyber acquisition is one area the Pentagon is not expected to cut as it trims $487 billion from DoD spending in the next 10 years. Frank Kendall, acting USD for AT&L said after a speech that his office is having trouble producing a report to Congress on how the Pentagon will acquire cyber warfare technologies [17]. Mr. Kendall explained that acquiring and testing cyber warfare equipment is not the same as purchasing other technology for the air and space domains. He also said that the cyber acquisition systems must move faster than the other programs in the air and space domains.

The primary objective of the DoD acquisition process is to acquire quality products that satisfy user needs with measurable improvements to mission capability and operational support, in a timely manner, and at a fair price [3]. Another perspective of DoD acquisition is that it exists to manage the nation's investments in technologies, programs, and product support necessary to achieve the National Security Strategy and support the U.S. Armed Forces [14]. The policies that govern the DoD acquisition system are intended to be flexible, responsive, innovative, disciplined, streamlined and effectively managed. The most discussed policies at this time are the "responsiveness" of cyber programs. Responsiveness is defined in DoDI 5000.1 as advanced technology that shall be integrated into predictable systems and deployed in the shortest time predictable [8]. Approved, time-phased capability needs matched with available technology and resources enable evolutionary acquisitions strategies. Evolutionary acquisition strategies are the preferred approach to satisfy operational needs. Incremental development is the preferred process for executing such strategies.

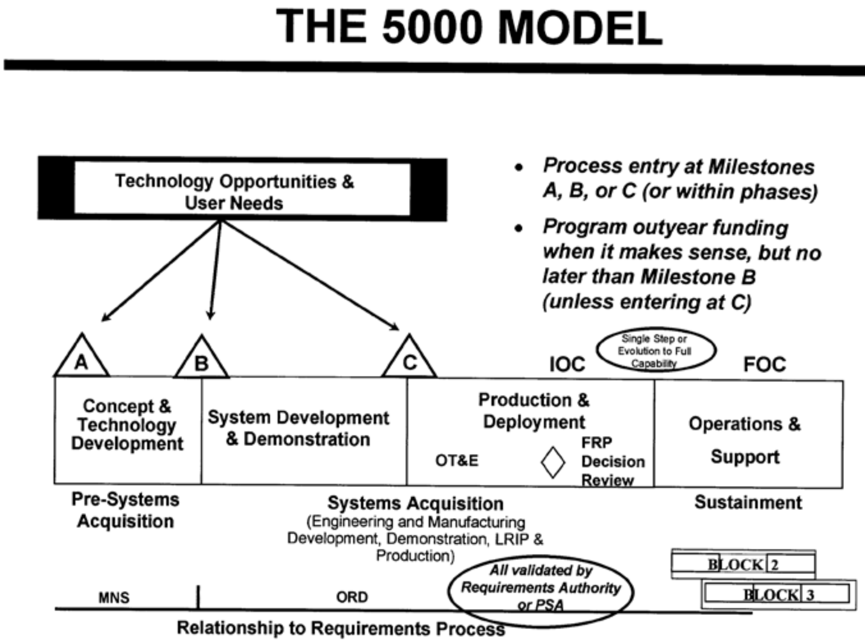

THE 5000 MODEL
Technology Opportunities & User Needs
Process entry at Milestones A, B, or C (or within phases)
Program outyear funding when it makes sense, but no later than Milestone B (unless entering at C)
A
B
C
IOC
Single Step or Evolution to Full Capability
FOC
Concept & Technology Development
System Development & Demonstration
Production & Deployment
OT&E
FRP Decision Review
Operations & Support
Pre-Systems Acquisition
Systems Acquisition
(Engineering and Manufacturing Development, Demonstration, LRIP & Production)
Sustainment
BLOCK 2
BLOCK 3
MNS
ORD
All validated by Requirements Authority or PSA
Relationship to Requirements Process

Figure 4 Defense Acquisition Management Framework [8]

Figure 4 delineates the traditional acquisition process into major miles stones indicated by the A, B and C. These three milestones represent different stages of the acquisition process to frame the management of the process. Milestone A is the point that presents authorization to the developer to enter into technology development which focuses on applying maturing technologies and allocating the requirements into subsystems, hardware, software and procedures. Milestone B is the point that authorizes the developer to enter into the system development and demonstration stage. This is the frame when the design documentation is complete. Milestone C is the point when the developer enters into production. Refer to Appendix D for more specific acquisition terms and definitions.

Defense acquisition management framework is guided by two DoD directives: DoDI 5000.1 and 5000.2 [3]. The directives apply to personnel within the DoD and to all acquisition programs. The purpose of the directives is to guide the management process by which the DoD provides effective, affordable, and timely systems to the users. The acquisition programs are directed, funded efforts that provide a new, improved, or continuing material, weapon or information system, or service capability in response to an approved need. Even “the highly classified, crytpologic, and intelligence projects and programs shall follow this guidance” [15]. The DoD instructions’ provide a higher-level view of the acquisition process and then the individual Services delineate them into Service specific instructions. For the AF there are three major instructions that apply:

- AFI 10-601 Capabilities Based Requirements Development – This instruction provides terms, definitions, methods, and measures to determine reliability, availability, maintainability, deployability, interoperability and other parameters which contribute to increased mission capability and supportability [19]. Many DAU certified professionals call this AFI the “ility” instruction.
- AFI 63-101 Operations of Capabilities Based Acquisition System – The purpose of this instruction is to implement direction from the SECAF as outlined in AF Policy Directive 63-1/20-1, Acquisition and Sustainment Life Cycle Management. The primary mission of the Integrated Life Cycle Management (ILCM) Enterprise is to provide seamless governance, transparency and integration of all aspects of weapons systems acquisition and sustainment management. This AFI must be used in conjunction with AFIs 10-601, Capabilities-Based Requirements Development, 99-103, Capabilities Based Test and Evaluation, 63-1201, Life Cycle Systems Engineering, and 20-101, Logistics Strategic Planning Procedures, to provide an integrated framework for the implementation of ILCM [20].
- AFI 99-103 Capabilities Based Test and Evaluation – This AFI discusses the overarching functions of test and evaluation (T&E). This is the main AFI that the operational test and evaluation (OT&E) community, such as the 346 test squadron (TS) for the cyber domain, abides by. T&E is used to mature system designs, manage risks, identify and help resolve deficiencies as early as possible, and ensure systems are operationally mission capable (i.e., effective and suitable). The AF T&E community plans for and conducts integrated testing as an efficient

continuum known as seamless verification in collaboration with the requirements and acquisition communities [21].

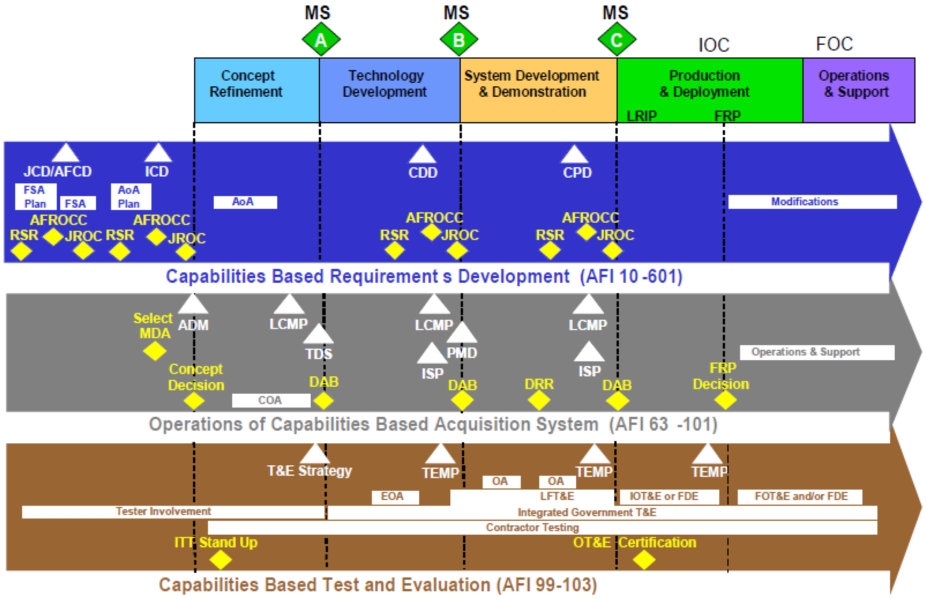


Figure 5 Air Force Acquisition Instructions [21]

Figure 5 shows a graphical depiction of the three AFIs discussed above. The depiction also notes the locations of the different milestones that were discussed for Figure 4. Refer to Appendix D for terms and definitions to the acronyms in Figure 5.

3.2 OT&E

OT&E determines if the requirements have been properly satisfied and assess the system for impacts to both peacetime and combat operations. OT&E identifies and helps resolve deficiencies as early as possible and evaluates changes in system configuration that could alter the system performance. Operational testing (OT) includes a determination of the operational impacts of fielding and/or employing a system across the full spectrum of military operations and may be conducted throughout the system lifecycle. OT may also look at doctrine, operational concepts (as described in AFPD 10-28, Air Force Operational Concepts), system performance, TTP, logistics support elements, intelligence support elements, system interoperability and security, materiel issues, safety, training, organization, human systems integration, and personnel [21].

An important aspect to keep in mind is the AF is purchasing cyber capabilities that are already in use in the commercial sector, called commercial-off-the-shelf (COTS). Many times a defense contractor will customize a COTS product for government use which is called government-off-the-shelf (GOTS).

3.2.1 Operational Test Organization

The organization within the AF that formally has the OT&E mission for cyber programs is the 346 TS in San Antonio, Texas. The 346 TS is the operational test organization (OTO) for AFSPC. An OTO is defined as an organization that is tasked to conduct OT&E within their respective MAJCOM. The programs are tested and thoroughly examined for strengths, limitation and vulnerabilities. The testers of the 346 TS provide detailed reports with recommendations to the 24 AF and AFSPC to determine if the tested equipment or capability may be deployed for operational use. If no testing is conducted, the systems might fail or introduce security vulnerabilities exposing the AF network to potential cyber threats. The 346 TS is the first line of defense ensuring new systems and capabilities meet the AF requirements for both the network and the warfighter [16].

3.2.2 AFOTEC

The air domain has been utilizing the process of T&E even prior to the AF being established in 1947. In the early 1940's, the Air Corps Proving Ground at Eglin AFB, Florida was stood up by General Henry "Hap" Arnold to assess the creation of aircraft and armament [10]. After the establishment of the AF the organization was renamed the Air Proving Ground Command (APGC) and was responsible for testing new aircraft in their operational roles as they rolled off the assembly lines. APGC conducted realistic testing of new weapons as an independent organization, reporting directly to the CSAF and advocating a "fly-before-buy" approach to acquiring new systems. Over the years the shift between "fly-before-buy" and "buy-fly-fix" plagued the AF and undervalued the importance of timely independent OT&E [10].

Fast-forward to the late 1960s when Deputy Secretary of Defense David Packard, the established entrepreneur who favored the "fly-before-buy" approach, and the Undersecretary of the Air Force John L. McLucas, who managed operational problems with the F-111 and C-5 transport, took the lead in defining a new emphasis on OT&E. On September 11, 1973, a directive from Headquarters AF established the Air Force Test and Evaluation Center that was to be based at Kirtland AFB, New Mexico.

In 1983, the Air Force added “Operational” to the Center’s name to more accurately describe the unique mission of evaluating the operational effectiveness and operational suitability of new systems. The name continues today as Air Force Operational Test and Evaluation Center (AFOTEC). AFOTEC is considered an operational test agency (OTA) since it conducts OT&E for the AF. As previously state, the OTO is the MAJCOM OT&E organization.

Today, AFOTEC has five detachments (Det), three operating locations (OL), and six liaison offices at locations across the U.S. AFOTEC continues to T&E new weapon systems and capabilities in operationally realistic environments. AFOTEC offers fact-based data in test reports to inform decision makers on a range of assessments of effectiveness, suitability, and whether a system is fully, partly, or not mission capable. For over 30 years, AFOTEC has been the focal point for AF OT&E and has significantly contributed to the successful acquisition and operational employment of numerous weapon and support systems for all branches of the armed forces, government agencies, and international allies [10].

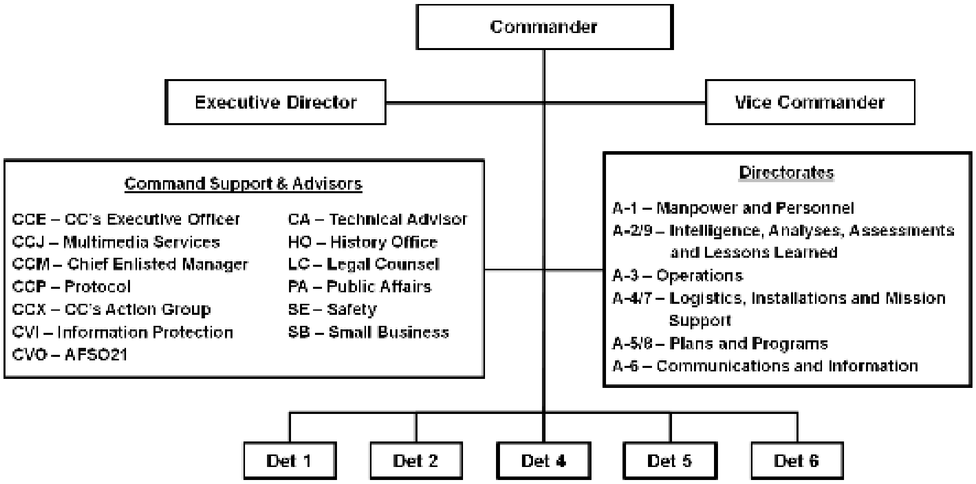

Commander
Executive Director
Vice Commander
Command Support & Advisors
CCE – CC's Executive Officer
CCJ – Multimedia Services
CCM – Chief Enlisted Manager
CCP – Protocol
CCX – CC's Action Group
CVI – Information Protection
CVO – AFSO21
CA – Technical Advisor
HO – History Office
LC – Legal Counsel
PA – Public Affairs
SE – Safety
SB – Small Business
Directorates
A-1 – Manpower and Personnel
A-2/9 – Intelligence, Analyses, Assessments and Lessons Learned
A-3 – Operations
A-4/7 – Logistics, Installations and Mission Support
A-5/8 – Plans and Programs
A-6 – Communications and Information
Det 1
Det 2
Det 4
Det 5
Det 6

Figure 6 AFOTEC Command Structure

In the past several years AFOTEC has undergone changes by closing several OLs and one Det. One of the implications of these changes left the cyber test domain in an unstable OT&E state. The responsibilities of cyber rest between Det 2 and 5 but primarily in Det 5 located at Eglin AFB, Florida. Examining the mission statements of the two Dets reveals no focus on the cyber domain; however, the air and space domain are explicitly indicated. Additionally, the Det 4 mission statement indicates “cyberspace and IT” OT&E; however, AFOTEC staffers stated this is accomplished by Det 2 and 5.

One of the major reasons for not having a cyber specific Det, which are discussed in the research section, is the cyber programs have not been listed as Acquisition Category (ACAT) I or is on OT&E oversight. ACAT I are programs are defined as programs that will require an eventual total expenditure for research, development, T&E of more than $365 million [2].

The following are mission descriptions and primary responsibilities for the AF’s major weapons systems:

- Detachment 1 (Det 1) is located at Edwards AFB, California, and has an OL at Fort Worth, Texas and Arlington, Virginia. Det 1 will lead Block 2 and 3 Initial OT&E for the joint strike fighter (JSF). The Det 1 commander serves at the Joint Strike Fighter Joint OT Team Combined Test Director, leading team members from the four Services and some international partners in T&E F-35 operations, training and logistics.
- Detachment 2 (Det 2) is located at Eglin AFB, Florida, and is one of the largest land-water ranges in the U.S. Det 2 tests new advanced munitions, electronic warfare equipment, mission planning systems, combat support, and command and control (C2) systems. Some of the systems tested by Det 2 include extended range Joint Air-to-Surface Standoff Missile, Air Intercept Missile 9X, the Small Diameter Bomb (SBD) II, Miniature Air Launched Decoy, and the Large Aircraft Infrared (IR) Counter Measure system.
- Detachment 3 (Det 3) – Deactivated on 5 April 2010 and was located at Eglin AFB, Florida.
- Detachment 4 (Det 4) is located at Peterson AFB, Colorado, and has an OL at Vandenberg AFB, California. Det 4 conducts OT&E on cyberspace, IT, missile and missile defense systems. Some of the major systems tested at Det 4 include Global Positioning System (GPS), Space Based IR Systems, Advanced Extremely High Frequency Satellite Communication, Space Based Space Surveillance, Cobra Judy Replacement, Defense Integrated Military Human Resource System, and the Integrated Strategic Planning and Analysis Network. In addition, Det 4 is part of the Ballistic Missile Defense System (BMDS) OT Agency Combined Test Force, supporting test events that evaluate components of the overall BMDS.

- Detachment 5 (Det 5) is located at Edwards AFB, California, and is co-located with the AF Flight Test Center. Det 5 also has an OL at Hurlburt Field, Florida. Det 5 performs OT&E of mobility, bomber, and C2, intelligence surveillance and reconnaissance (ISR) weapon systems. Det 5's major test programs include the C-5M Super Galaxy, MQ-9 Reaper, RQ-4 Global Hawk, C-130 enhancements and ongoing system upgrades to the B-1, B-2, and B-52 bomber test fleet. Additionally, Det 5 manages OT of the following: Common Vertical Life Support Platform, C-27J Joint Cargo Aircraft, E-3 Sentry Airborne Warning and Control System and KC-46 tanker program.
- Detachment 6 (Det 6) is located at Nellis AFB, Nevada., near the Nevada test and training range (NTTR). Det 6 conducts OT&E of currently fielded AF fighter aircraft. Det 6 programs include the F/A-22 Raptor, A-10C Thunderbolt II, F-16C Fighting Falcon, F-15C Eagle, and F-15E Strike Eagle.

3.2.3 Cyber Ranges

This section discusses the use of cyber ranges for verifying and validating acquisitions and TTP. Successful acquisition depends on the availability of suitable infrastructure. Cyber ranges are highly considered the most cost effective way to validate new TTPs. There have been significant DoD investments into the cyber ranges, for example, the National Cyber Range, the Navy/Marine Corps Cyber Information Assurance Range, the Joint Information Operations Range and the Air Force Research Laboratory (AFRL) Cyber Experimentation Environment

The uses of cyber test ranges are used to leverage separately encrypted, closed loop enclaves over various DoD and U.S. Federal networks. The closed loop is achieved through cryptographic isolation using hardware encryptors uniquely keyed. Inside that closed loop all traffic is further segregated and isolated via local logical ranges using dedicated Internet protocol security virtual private networks. The closed network can operate at any security level or at multiple security levels simultaneously from secret to top secret. The ranges intent to help mitigate the risks associated with the development, assessment, and the testing of emerging and mature cyber capabilities. The cyber ranges can be found within U.S. military Services and agencies, at other government units as well as at private industry installations [9].

3.3 AF TENCAP

Air Force Tactical Exploitation of National Capabilities (AF TENCAP) has been bridging the gap between organizations such as the central intelligence agency, defense intelligence agency, national reconnaissance office, NSA and the tactical warfighter since 1977. The purpose is to provide the best, most accurate and timely information and data possible to those going into harm's way. In the last thirty years, approximately 150 programs have been examined, of which roughly 68 were transitioned to the user. The small, lean organization has the capability of putting programs together in three to 12 months, depending on the complexity costs, and available technologies [14]. Note that AF TENCAP is not an OT&E organization that does verification and validation like AFOTEC or the 346 TS.

Colonel Robert "Bob" Wright, commander, commander of the Space Innovation and Development Center (SIDC) said the bottom line of AF TENCAP "is they execute quickly to support the warfighters in the field" [15]. He went on to say "bringing capabilities to the combatant commanders is the bottom line. They have about 53 projects working at any one time. Of those projects, 37 have ties to the national intelligence agencies in Washington, D.C." [15].

The organization is lean with only 30 active duty officers, enlisted, and civilians, along with additional contractors and a budget of $12 million a year. When AF TENCAP gets assigned a project, the team asks the requestors to provide funding so they can maintain the fast turnaround needed to support combatant commanders' needs. One specific program is the Talon Namath program which was based on extremely accurate GPS location capabilities to be used by the SBD that the Joint Forces Air Component Commander wanted to have in theater as soon as possible.

It is important to point that not one of these programs falls within the rapid acquisition process.

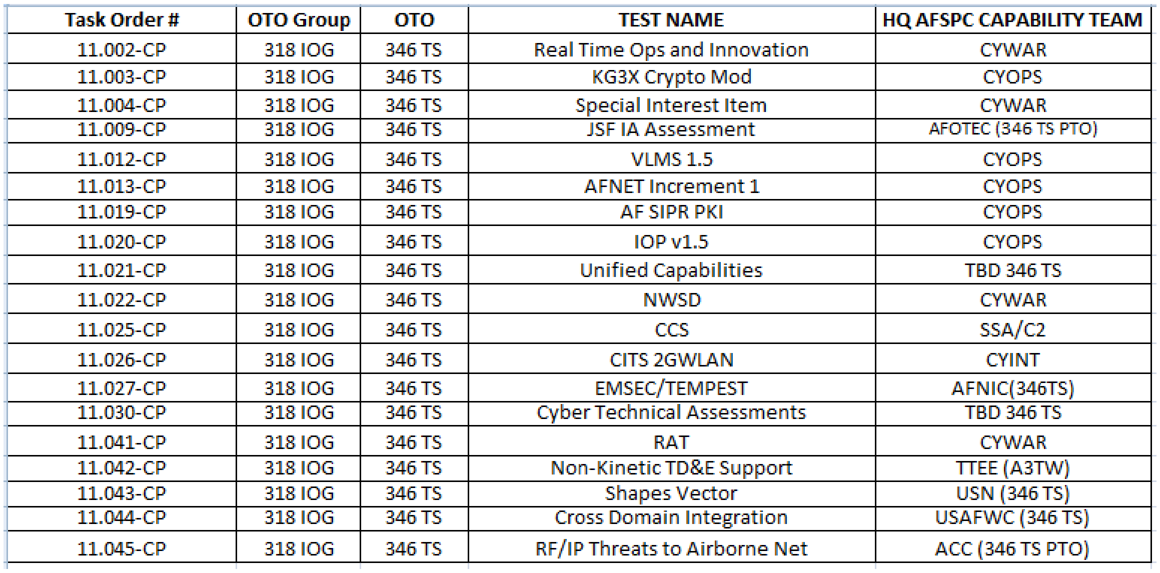
3.4 Test Priority List

The test priority list (TPL) is a comprehensive, prioritized list of all AFSPC's approved operational and integrated test asset support activities conducted. The TPL sets the relative priority of projects for the OTO within AFSPC and servers as a guide for allocating resources, such as personnel and financing. The TPL also provides authorization and direction to execute testing on the programs.

When a new program is approved for testing it is placed on the TPL, which in turn provides the responsible test organization (RTO) approval and priority if there becomes a dilemma in regards to time, assets, and/or money. The RTO for cyber within AFSPC is the 346 TS which are also known as the OTO. Take note in Table 1 and 2, only the 346 TS is delineated since the listed programs were secluded from the AFSPC TPL which would have included the space programs.

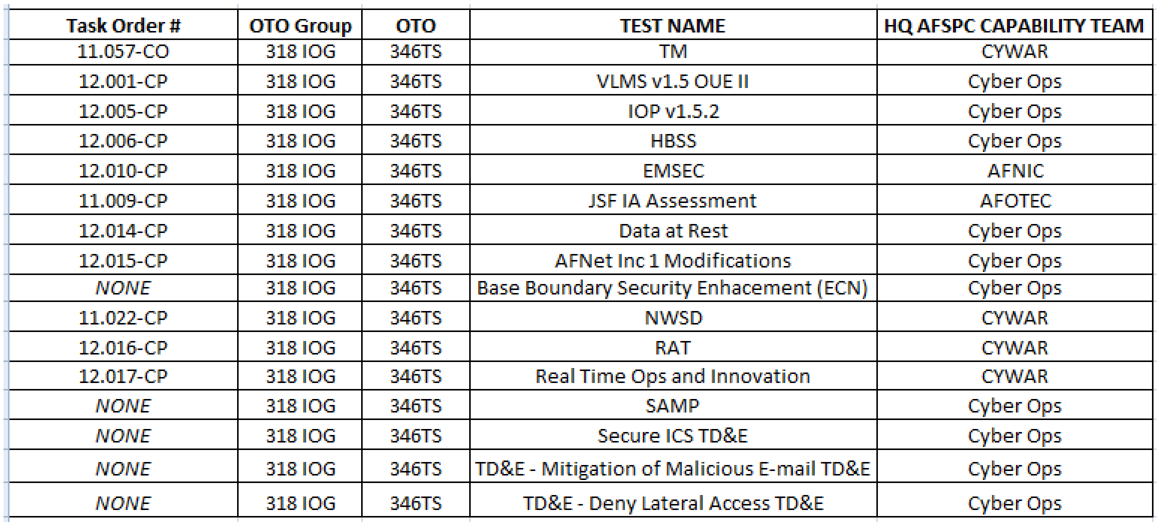
Since the establishment of AFCYBER, there have only been two approved TPLs in the FY 2011 and 2012. Prior to 2011, there was a consolidated test list or CTL, which incorporated space programs. Note that some programs are listed in both FY11 and FY12 (see Table 1 and 2). This is because the programs are long enduring or developed in multiple phases.

Table 1 FY11 AFCYBER Test Priority List



Task Order #	OTO Group	OTO	TEST NAME	HQ AFSPC CAPABILITY TEAM
11.002-CP	318 IOG	346 TS	Real Time Ops and Innovation	CYWAR
11.003-CP	318 IOG	346 TS	KG3X Crypto Mod	CYOPS
11.004-CP	318 IOG	346 TS	Special Interest Item	CYWAR
11.009-CP	318 IOG	346 TS	JSF IA Assessment	AFOTEC (346 TS PTO)
11.012-CP	318 IOG	346 TS	VLMS 1.5	CYOPS
11.013-CP	318 IOG	346 TS	AFNET Increment 1	CYOPS
11.019-CP	318 IOG	346 TS	AF SIPR PKI	CYOPS
11.020-CP	318 IOG	346 TS	IOP v1.5	CYOPS
11.021-CP	318 IOG	346 TS	Unified Capabilities	TBD 346 TS
11.022-CP	318 IOG	346 TS	NWSD	CYWAR
11.025-CP	318 IOG	346 TS	CCS	SSA/C2
11.026-CP	318 IOG	346 TS	CITS 2GWLAN	CYINT
11.027-CP	318 IOG	346 TS	EMSEC/TEMPEST	AFNIC(346TS)
11.030-CP	318 IOG	346 TS	Cyber Technical Assessments	TBD 346 TS
11.041-CP	318 IOG	346 TS	RAT	CYWAR
11.042-CP	318 IOG	346 TS	Non-Kinetic TD&E Support	TTEE (A3TW)
11.043-CP	318 IOG	346 TS	Shapes Vector	USN (346 TS)
11.044-CP	318 IOG	346 TS	Cross Domain Integration	USAFWC (346 TS)
11.045-CP	318 IOG	346 TS	RF/IP Threats to Airborne Net	ACC (346 TS PTO)

Table 2 FY12 AFCYBER Test Priority List



Task Order #	OTO Group	OTO	TEST NAME	HQ AFSPC CAPABILITY TEAM
11.057-CO	318 IOG	346TS	TM	CYWAR
12.001-CP	318 IOG	346TS	VLMS v1.5 OUE II	Cyber Ops
12.005-CP	318 IOG	346TS	IOP v1.5.2	Cyber Ops
12.006-CP	318 IOG	346TS	HBSS	Cyber Ops
12.010-CP	318 IOG	346TS	EMSEC	AFNIC
11.009-CP	318 IOG	346TS	JSF IA Assessment	AFOTEC
12.014-CP	318 IOG	346TS	Data at Rest	Cyber Ops
12.015-CP	318 IOG	346TS	AFNet Inc 1 Modifications	Cyber Ops
NONE	318 IOG	346TS	Base Boundary Security Enhacement (ECN)	Cyber Ops
11.022-CP	318 IOG	346TS	NWSD	CYWAR
12.016-CP	318 IOG	346TS	RAT	CYWAR
12.017-CP	318 IOG	346TS	Real Time Ops and Innovation	CYWAR
NONE	318 IOG	346TS	SAMP	Cyber Ops
NONE	318 IOG	346TS	Secure ICS TD&E	Cyber Ops
NONE	318 IOG	346TS	TD&E - Mitigation of Malicious E-mail TD&E	Cyber Ops
NONE	318 IOG	346TS	TD&E - Deny Lateral Access TD&E	Cyber Ops

On the right side of the TPL there is a list of the capability teams or lead organization for the program. An example lead organization is AFOTEC. AFOTEC is the AF lead for information assurance testing of the JSF but they currently do not possess the SMEs to conduct OT&E, so they leverage the 346 TS. The capability teams are comprised of the staff organizations within AFSPC. For example, the programs listed under “test name” are categorized into cyber operations or cyber warfare. The teams have staff level action officers that participate on the development of the program. The action officers reside from A2 (Intelligence), A3 (Operations), A5 (Plans), A8 (Requirements), and other additional areas.

3.5 Programs

Up to this point the discussion has centered on only PoRs, defined as a program which has prevailed the POM process and is listed as a FYDP. With that said, there is a clear delineation between a PoR and other program initiatives like AF TENCAP that are trying to fill technology gaps within strategic and tactical level PoRs so they can be better utilized by more DoD personnel. This section provides several examples of each type of program to demonstrate a clear delineation between the two. The most important factor is a PoR has dedicated funding for the program and sustainment. In many instances, cyber programs lack sustainment funding or adoption from other PoRs.

Example PoRs:

1. Combat Information Transport System (CITS) portfolio is a family of programs that incorporate a variety of COTS/GOTS items that must be integrated to perform the required military missions.
2. Air Force Network (AFNet) is both a network defense and network management tool to manage the web and email operations as one. The AF has been testing this program in a incremental approach.
3. Host Based Security System (HBSS) is a COTS/GOTS suite of software applications to monitor, detect and counter attacks against the DoD computer network and systems.

Example program initiatives would be ones that transpired out of AF TENCAP like the "Talon" series of programs. One "Talon" program example is Talon Namath which helped improve the GPS delivery accuracy of SDBs. Another example would be the Talon Shield which is based off space-based on early warning for missile launches [15]. There are more program initiative examples but to preserve this research as unclassified the specifics of each program initiative are not documented.

AF TENCAP is only one example of an organization trying to advance cyber capabilities. Another organization is the defense advanced research projects agency (DARPA) which is responsible for advancing new technology for use by the DoD. The mission of DARPA is to prevent technological surprise to the U.S. and to create surprise for its enemies. Yet another example is the AFRL which is dedicated to leading the discovery, development and integration of new technologies to the AF. Both of these organizations are working on developments that at some point may or may not become a PoR during their program life cycle.

3.6 OSD Oversight

Every year in accordance with DoD instruction 5000.2 (Operation of the Defense Acquisition System), OSD identifies programs that are listed on the T&E oversight list [8]. The list specifies developmental, operational, and live-fire T&E oversight requirements for each program. Each year the list supersedes all previous versions of the OSD T&E oversight list. The list does not include highly classified and sensitive programs subject to T&E oversight, which are identified directly to the program mangers. Note, the only cyber PoR on OSD oversight is CITS.

3.7 Summary

This chapter explained the complexity of the acquisition process currently used today. The chapter discussed many of the organizations within the AF that test, validate and verify cyber programs. Examination of PoRs and ongoing efforts of the associated units failed to identify any specific requirements for delivery of a cyber capability via rapid acquisition process. This next chapter will open the aperture to look outside of acquisitions and examine TTP for delivery of rapid cyber capabilities.

IV. Tactics, Techniques & Procedures

"We do a lot of information sharing. We do very little collaboration. There is a great deal of information that is out there concerning threats, as well as tactics, techniques and procedures to inoculate our different networks such that they would not be attacked or would not be penetrated. And if they were and are, we would be able to do something about it" [28].

Major General Ronnie D. Hawkins Jr.
Vice Director of Defense Information Systems Agency

Exploits disrupt or manipulate data systems in an attempt to target vulnerabilities. The effects can disable businesses, financial institutions, medical institutions and/or government agencies. For example, an exploit could alter credit card transaction data on an e-commerce website for a financial gain or manipulate financial data to erode public confidence in that bank. In short, a cyber exploit has the potential to create extreme damage that is generally significant relative to the low cost of initiating the attack. This chapter examines rapid delivery of capabilities via TTP.

4.1 AFSPC TTP Program

The AFSPC Tactics Development Program is designed to meet AFSPC's responsibility to serve as the lead command in developing, documenting, and issuing Air Force tactics, techniques and procedures (AFTTP) for space and cyberspace weapons systems per AFSPC instruction 10-260 [36].

AFSPC uses the Tactics Development Program to improve the combat capabilities of AF weapon systems and how they integrate into the joint fight. Note that the definition of a cyber weapons system is still in discussion within the cyber community. In the air and space domains there is a clear delineation of what constitutes a weapon system.

AFSPC Tactics Development Program goals:

- Improve overall military capability by instituting a responsive, standardized process to identify and address areas for improvement in AFSPC operations, systems, support, and C2.
- Integrate tactics and intelligence considerations into daily operations and training.
- Rapidly validate and disseminate new tactics to correct deficiencies or pursue new/improved AFTTP.

- Persistently verify existing tactics against emerging threats and technologies.
- Invigorate the AFSPC tactics process, resulting in a robust program that not only improves organic weapon system effectiveness but leads to better integration with other MAJCOM tactics development processes.
- Facilitate the development of new AFTTP based on weapon system modifications to leverage new hardware, software, and operator capabilities.

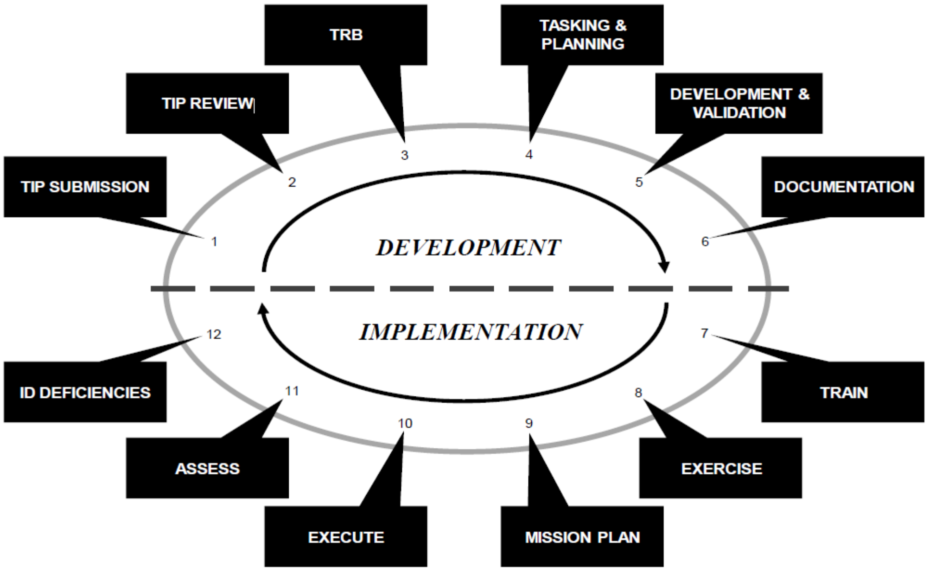


Figure 7 Tactics, Techniques, & Procedures Cycle [36]

Figure 8 demonstrates the TTP cycle. For purposes of this research, focus is on the section above the dashed line associated with development.

The six steps below are the focus on cyber TTP development:

1.) TIP Submission – The tactics improvement proposal (TIP) is an idea to improve a capability of an existing fielded system, to overcome a tactical deficiency, or meet an emerging operational need. The TIP is submitted on AF Form 4326, Tactics Improvement Proposal, 29 September 2011which is provided in Appendix B [36]. TTP are for non-material solutions.

2.) TIP Review – The first vetting process to make sure that the submitted TIP meets the criteria established in AFI 10-260 and AFSPCI 10-260 [22].

3.) TRB – The Tactics Review Board (TRB) is a formal conference that is established to vet the submitted TIPs. Within the TRB are normally separate working groups (WG) that investigate the different mission areas (MA) such as network defense or attack. Note that, there are several TRBs, within the AF.

4.) Tasking & Planning – Once the TIPs have been approved at the TRB they are tasked to the 688 Information Operations Wing (IOW). From this point they are listed on the AFSPC TPL and tasked to the respective RTO which in the case of cyber would be the 346 TS. The primary means for conducting tactics development is via a tactics development and evaluation (TD&E) or a tactics development initiative (TDI) which is covered in more detail in Section 4.2.

5.) Development & Validation – The organizations that have been tasked help develop the requirements and estimated costs for the tactics development.

6.) Documentation – Once the development and validation is complete it is documented and sent to the 561 JTS for AFTTP approval and dissemination.

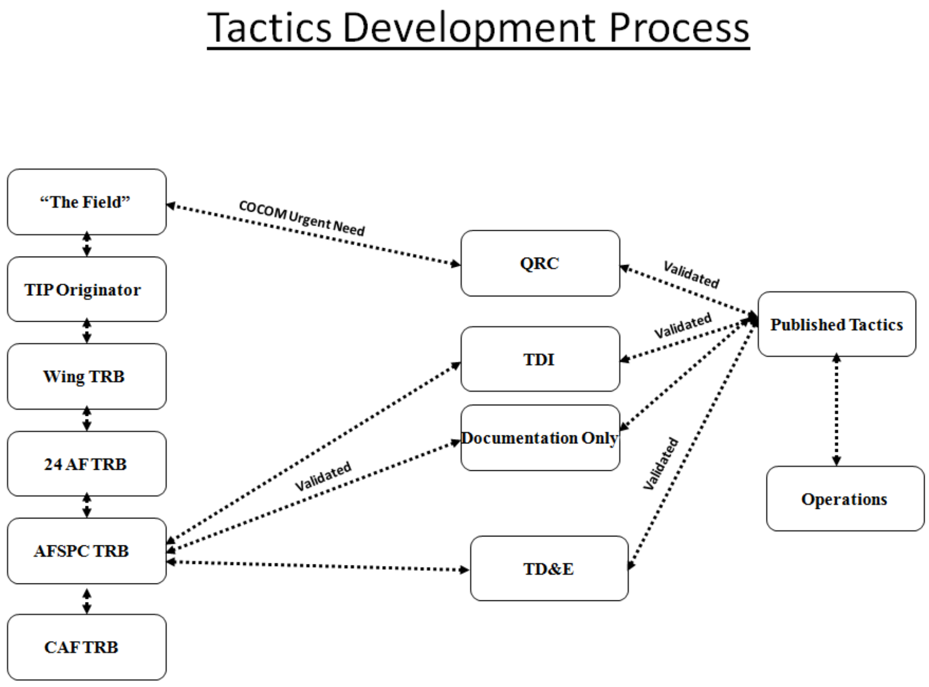


Figure 9 Tactics Development Process

Figure 9 is the Tactics Development Process. It is a step-by-step process that demonstrates organization roles. "The Field" is considered those organizations that are involved in operations supporting contingencies. Those organizations have the ability to submit an urgent operational need (UON) or joint urgent operational need (JUON). These two submission processes are used to decrease the timeline of providing a capability to "The Field." The solution to the UON and/or JUON is usually a quick reaction capability (QRC). The guidance on QRCs is outlined in AFI 63-144, Quick Reaction Capability Process [40].

A major recent change incorporates an AFSPC commander approved memorandum on Real-Time Operations and Innovation (RTO&I). The construct of the memorandum establishes roles, responsibilities, processes, and authorities for executing RTO&I within AFSPC. This new construct enables the AF to generate capabilities to address critical cyber needs as the needs arise. As stated previously the process to address the critical cyber needs is to use the CNF which is in Appendix A. This requires a dynamic, agile, risk-based approach, balancing the needs against the operational risks and threats. The memorandum is intended to be complementary to the traditional acquisition framework and is primarily focused on tools and/or tactics that bring a new capability to the 24 AF.

The memorandum replaces the use of ACC instruction 63-250. AFSPC has been mirroring the ACC construct for quite some time as an outline on how to conduct rapid acquisition within the air domain.

4.2 AFSPC Operational Test Organization

As stated previously the 346 TS is AFSPC's OTO tasked for conducting OT in the cyber realm. One of the unique test methods within OT is the deployment of tactics based on the information derived from a TD&E. TD&Es are a tailored type of Force Development Evaluation (FDE) conducted by MAJCOMs to refine doctrine, system capabilities, and TTP throughout a system's life cycle. TD&Es identify non-materiel solutions to problems or evaluate better ways to incorporate into new or existing systems. The TD&E is a much more rigorous methodology for developing tactics versus the TDI [36].

4.3 318th Operational Support Squadron

The 318th Operational Support Squadron (OSS) is the only organization within AFSPC that is tasked with conducting TDIs. TDIs are tactics development and validation efforts executed by the 688th IOW and SIDC using organic resources. TDIs provide a flexible capability to remain responsive to rapid changes in current and emerging cyber tactics. They provide a higher level of fidelity than that achieved via exercises, but less than that achieved via formal testing. They may be developed and executed by SMEs, engineers, and testers using a test-like approach; however, TDIs are not considered formal testing as defined in AFSPCI 99-103, Capabilities-Based Test and Evaluation of Space and Cyberspace Systems [24]. The TDIs are less intensive and are “low to medium development effort” compared to a TD&E. Note that the 318 OSS is not considered an OTO like the 346 TS.

4.4 Joint Tactics Squadron

The 561st Joint Tactics Squadron (JTS) has the mission to gather, facilitate and disseminates TTPs. The 561st is based out of Nellis AFB, Nevada and was stood up in 2006 to create a more adequate cycle for updating TTP in today’s fast-paced, dynamic environment [23].

When the 346 TS or 318 OSS complete a TD&E or TDI they document the findings and provide them to the cyber SME at the 561 JTS so it can be documented in a flash bulletin (FB) or tactics bulletin (TB). The FB and TB can be later combined and recorded in AFTTP 3-1 or 3-3. AFTTPs are reevaluated every one to two years per the guidance established in AFI 11-260 [22].

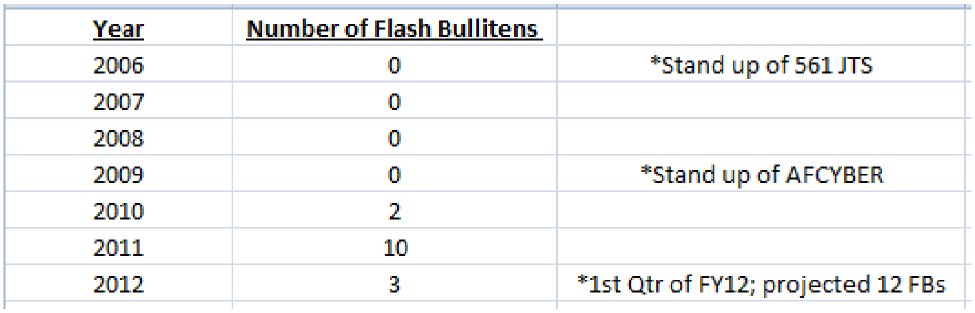
There are three types of documentation that the 561 JTS facilitate:

1. AFTTP 3-1/3-3 series volumes – Comprehensive tactical weapon system employment manuals. The volumes describe specific TTP employed by the weapon system operator to deliver desired effects. These documents are typically reviewed every 2 years or deemed appropriate by headquarters AFSPC/A3. The delineation between an AFTTP 3-1 and AFTTP 3-1 is their security classification.
2. Tactic Bulletin (TB) – Act as official AFTTP 3-1/3-3 series volumes between rewrites in an effort to ensure the AFTTP remain current. TBs cannot alter the guidance from AFTTP but can

expound upon the existing material. When it is time to review AFTTP the TBs are incorporated as appropriate.

3. Flash Bulletin (FB) – Are usually lessons learned that are time sensitive and need to be distributed to the warfighter immediately. The FBs are approved and published by the 561 JTS commander. FBs can become TBs after more comprehensive vetting, and should be incorporated into future AFTTP 3-1/3-3 rewrite when applicable.

Table 3 561 JTS Published Flash Bulletins



Year	Number of Flash Bullitens	
2006	0	*Stand up of 561 JTS
2007	0	
2008	0	
2009	0	*Stand up of AFCYBER
2010	2	
2011	10	
2012	3	*1st Qtr of FY12; projected 12 FBs

Table 3 indicates the number of FBs created over the past several years. The names and the specifics of the FBs are classified and posted on the 561 JTS secret Internet protocol router network (SIPRNet) website.

4.5 Air Land Sea Application Center

The Air Land Sea Application (ALSA) Center is the organization within the DoD that is chartered for creating and developing multi-service tactics, techniques and procedures (MTTP). ALSA's mission is to develop publications, studies, periodicals and other solutions across the entire military spectrum to meet the immediate needs of the warfighter. These projects provide solutions that address interoperability issues to meet the immediate needs of operating forces or to fill gaps in existing TTP. ALSA provides a unique capability, tailored to the warfighter's needs, to develop products that coordinate TTP between the Services and complement other efforts of government, joint, and Service staffs [41].

The following requirements must be met in order for ALSA to develop a project:

- Two or more Services agree to actively participate in the project. The agreement between all four Services is preferable.

- No Service objects to ALSA's participation in a project.
- The project is supported by SMEs, operators, and users from each of the participating Services.
- The project does not contradict joint doctrine, both published and under development.
- The project must be independent of, but may be in coordination with similar efforts by other staff agencies.
- Resources are available to support the project (e.g., personnel, funding, time).

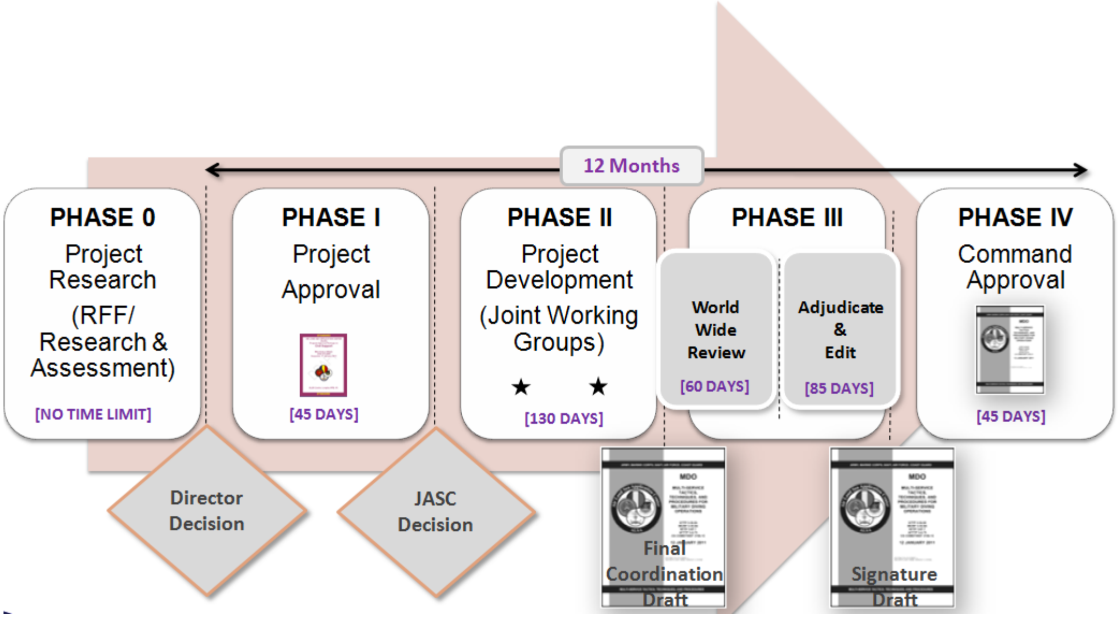


Figure 8 ALSA's MTTP 12-Month Cycle Phases [41]

Figure 9 shows the 12-month cycle when a new MTTP is proposed to ALSA. The cycle shows the complexity of the development and approval phases needed in the creation.

The MTTP documents are revised every two to three years. There is a long term schedule that is distributed by ALSA for planning purposes. The schedule lets other organizations know when they can help contribute to the next editions of an MTTP. Ideas to generate a new MTTP can be submitted at any time throughout the year.

4.6 Joint Test and Evolution Program

The Joint Program Office (JPO), located in Suffolk, Virginia, is the administrators of the Joint Test and Evaluation (JT&E) Program. The JT&E Program involves two or more military Services, Combatant Commands (COCOM), Joint Chiefs of Staff (JCS), and other DoD agencies to solve joint problems with non-materiel solutions. The JT&E Program is used to assess service interoperability, analyze joint military capabilities, develop potential options for increasing joint military effectiveness, and improve joint TTP. The guidance for JT&Es is in AFI 99-106, Joint Test and Evaluation Program, 26 August 2009 [35].
The JT&E Program purpose is to:

- Assess Service system interoperability in joint operations and explore potential solutions to identified problems.
- Evaluate joint technical and operational concepts and recommend improvements.
- Validate testing methodologies that have joint application.
- Improve modeling and simulation (M&S) validity with field exercise data.
- Increase joint mission capability using quantitative and qualitative data for analysis.
- Provide feedback to the acquisition and joint operations communities.
- Improve joint and MTTPs.

The JT&E Program consists of two levels of efforts: Joint Tests (JT) and Quick Reaction Tests (QRTs).

QRTs are one-year test efforts also funded by OSD. QRTs address specific and focused joint warfighter questions or issues within the scope of the JT&E Program's purpose. Services, COCOMs, Joint Staff, or other DoD agencies may sponsor QRTs. Sponsoring organizations, assisted by the QRT team and AFJO, will define desired products from the QRT effort. QRTs nominations can be submitted to Air Force joint test and evaluation program office (AFJO) anytime and are typically vetted by the Services, Joint Staff and COCOM at JPO sponsored WGs. Urgent QRTs typically require high level (Four-star) sponsorship and endorsement. The AFJO is the conduit into the JPO, which is the facilitator for submitting the nominations of JT and QRTs.

4.6.1 Quick Reaction Test

QRT nominations address the following:

- Joint military operational critical issues affecting combat operations and capabilities. These issues can be derived from on-going combat operations and recurring Joint Staff and COCOM issues and lessons learned conferences.
- Joint transformational issues raised through Joint Staff.
- Joint issues identified from COCOM field assessments and tactical operations.
- Issues generated from other JT&E projects.
- Joint operational issues that are spin-offs from advanced joint concept technology demonstrations (JCTD) or joint experiments. The definition of a JCTD and numerous other terms are in Appendix D.

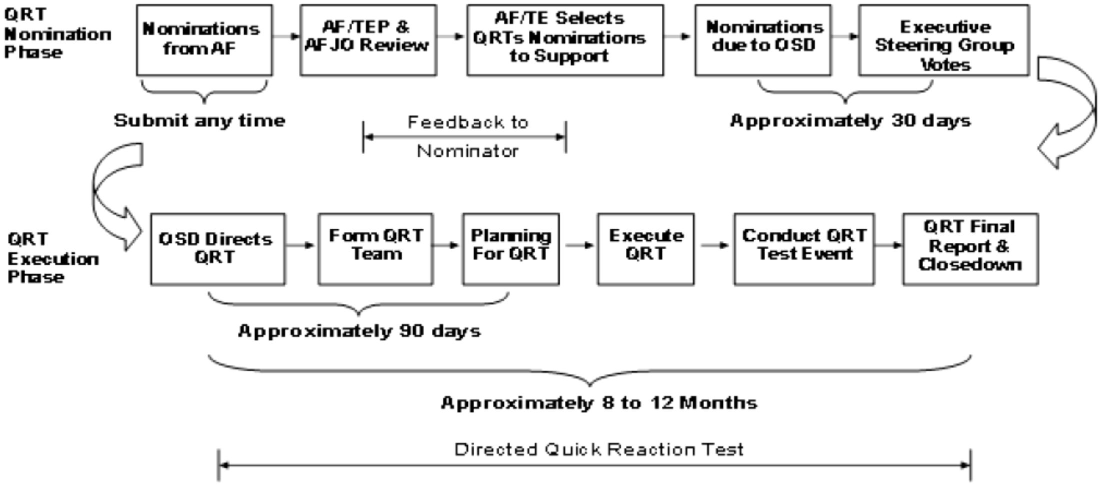


Figure 9 QRT Phases [35]

There are two phases to the QRT; the nomination and execution phase. Below is an explanation of each:

- QRT Nomination Phase - The nominating organization within a MAJCOM will notify AFJO and AF/TEP of the intention to submit a QRT nomination. The nomination organization QRT will also provide resource requirement estimates to AFJO. AFJO and AF will determine if the proposed solution to the problem meets the criteria for a QRT.

- QRT Execution Phase - Initial QRT planning starts with the nominating organization developing the Project Master Plan with assistance from AFJO and the joint steering committee (as available). The nominating organization will prepare a Project Test Plan within 60-days of being directed by the OSD.

4.6.2 Joint Test

Joint Test (JT) projects are longer efforts lasting up to three years. JT projects are composed of three sequential phases: JT Nomination Phase; Joint Feasibility Study (JFS) Phase; and JT Execution Phase.

- JT Project Nomination Phase - Organizations prepare JT nomination packages each year in the format specified by OSD. A well-defined purpose and problem statement with joint implications is critical since it is the basis for prioritizing need, relevancy, and determining basic test feasibility. Successful nominations secure two or more general officer advocates with endorsements from the services and COCOMS.
- JFS Phase - The JFS determines whether a JT project nomination is operationally and technically feasible to resolve a joint problem. JFS duration is short (seven-months or less). The Figure 10 shows the events with this phase.
- JT Project Execution Phase. After OSD issues a chartering document, a JT project is required to be completed within three-years. JT projects are conducted in realistic joint operational environments where possible. JT projects are frequently conducted in conjunction with joint exercises (subject to approval), and may be supplemented by M&S if field test and joint exercise data is not available. Timing of joint exercises during the JT&E execution phase may drive test planning significantly.

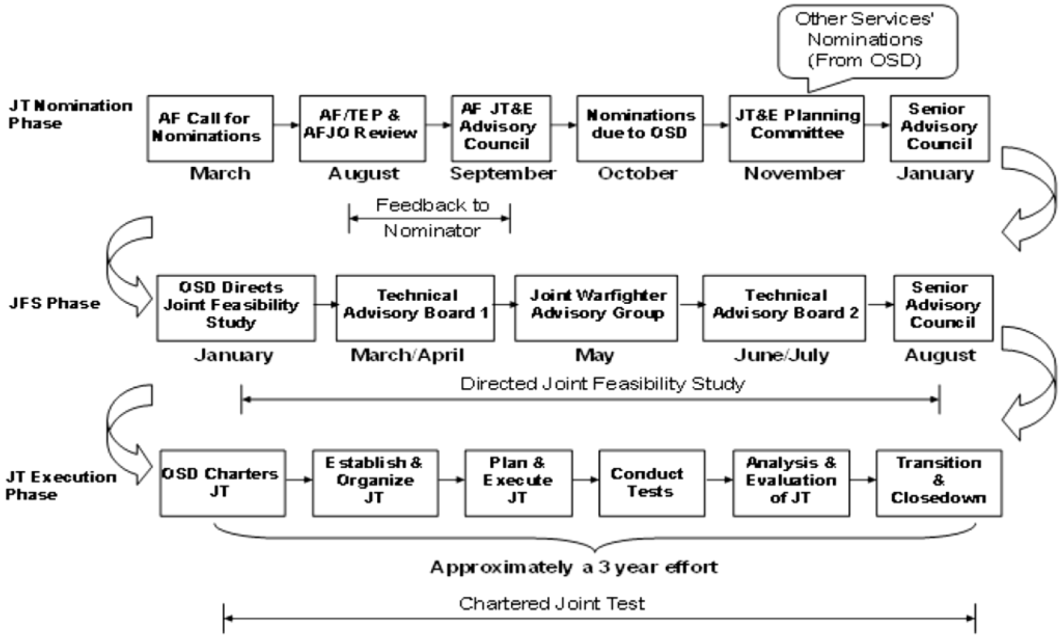


Figure 10 JT Phases [35]

4.6.3 Current JT and QRT

Currently, the JT&E office has approved a one-year QRT called Joint Threat Assessment and Negation for Installation Infrastructure Control Systems (JTANIICS). The JTANIICS QRT is directed to develop and validate a risk assessment tool that gives installation commanders the following:

- The ability to conduct self-assessment of industrial control systems (ICS) vulnerabilities subject to intrusion from unauthorized external sources.
- The ability to prioritize the application of resources toward the assessed vulnerabilities based on mission requirements.

The QRT scope is limited to using the non-secure Internet protocol router network (NIPRNet). JTANIICS will generate a TTP document for commanders of DoD installations and operating bases to assess their ICS for susceptibility to cyber-based intrusion and develop correction or contingency plans to meet mission needs [24].

The JT&E office has also approved a three-year JT called Joint Cyber Operations. The JCO JT is chartered to employ multiservice and other DoD agency support, personnel, and equipment to assess, develop, and evaluate adaptive cyber defense TTP used to employ a virtual secure enclave strategy to ensure the protection and availability of critical C2 services. The JCO JT will focus the TTP development and refinement on improving computer network defense of critical C2 services in support of the joint task force commanders in an operational environment [25].

4.7 Summary

TTP depend on continuous refinement, review of intelligence and inputs from operational units. The next chapter analyzes the requirements for rapid acquisition based on current capability delivery and requirements.

V. Analysis & Discussion

This chapter analyzes and findings associated with rapid capability delivery. This chapter will also investigate process considerations, cyber organizations and lastly the on-going cyber venues within the AF.

5.1 Process Considerations

5.1.1 Time

In regards to combat domains, history has proven that in due time difficulties associated with emerging technologies resolve themselves. That is said based on all the activity that is transpiring within the cyber realm. Consider for example when the Army created the Air Corps. Decades later the space domain was added and had to struggle with some of the same things as the air domain. Now cyberspace has emerged as a new war fighting domain and is facing some of the same identity struggles. Currently there is strategic DoD guidance, such as NDAA, that is being enacted to set the tone for more specific rules and regulations on the rapid acquisition of cyber programs. As laws and regulations that provide the construct to the military doctrine become more solidified at a DoD level, it will incidentally unfold and serve as guidance for the joint environment like USCYBERCOM.

Most recently General Martin Dempsey, Chairman of the Joint Chiefs of Staff (CJCS), recommended a change to transition the two-year old USCYBERCOM to a full combatant command status [28]. The elevation of USCYBERCOM to a level on a par with commands protecting entire regions and continents would give the nation’s top cyber warriors more direct access to CJCS and Sec Def, allowing more clout in the struggle for resources [29]. This will also send a signal to adversaries that the DoD is serious about protecting its ability to operate in cyberspace. With that said, a concern is that USCYBERCOM has only 750 people assigned, far fewer than the other combatant commands. How realistically can a COCOM move forward without the proper training, personnel and budget? To answer the third issue, Defense Secretary Panetta said cyber will not be subject to the Pentagon’s attempt to reduce the DoD budget by $487 billion over the next decade. However, there are cost cutting measures in place that will reduce military personnel significantly. Within that debate is if the troop reduction will come from the air national guard, reserves or the active duty.

5.1.2 Acquisitions

Cyber acquisitions from a historical perspective have not had any PoRs developed and fielded in the time frame which is considered to be rapid. Some leaders, however desire cyber initiatives with delivery to the AF network within weeks to months. Indeed some claim the cyber acquisition process needs to be able to react faster and produce capabilities within a shorter duration; however, the CITS program was recently put on the OSD oversight list which will create a lengthier time frame for approval of the capability. This action actually slows the acquisition and fielding process. It also means cyber programs designated for OSD oversight are going to be subject to the provisions of Title 10 of U.S. Code 139, 2366, 2399, 2400 and the requirements of DoD Instruction 5000.2 for T&E Strategies, System, Threat Assessments, Test and Evaluation Master Plans, Developmental and OT&E Plans, and reporting all results and milestone to OSD. CITS is known to be a large portfolio of numerous programs and is why it is consider an ACAT I program (e.g. more than $365 million) . There is also discussion of dividing the CITS program into smaller ACAT categories to lessen the oversight and regulations that accompany them.

Not surprisingly, many problems stem from the issue of funding. Many of the staff officers contacted in the phase one of this research said the cyber community as a whole was having trouble communicating the proper requirements to the higher echelon of leadership that approve funding. That could be the reason for the numerous programs that are aligned under the CITS program.

That right balance may stem from a new DoD mandated strategy that outlines a process for rapid acquisition of tools, applications, and other capabilities for cyber warfare for CYBERCOM. This new strategy is called the “Strategy for Acquisitions and Oversight of DoD Cyber Defense Capabilities” and is contained within NDAA that draws significant lines between what is rapid and deliberate [1].

Recently, the cyber acquisition community incorporated a unique method to deliver requirements via the CNF. The CNF captures the capability to alleviate any ambiguity of the nature of the cyber requirements. The air and space domain are without this type of process and this research did not examine if this process was beneficial to the cyber community [36]. The current CNF is in Appendix A.

5.1.3 TTP

When contacted, many personnel did not clearly understand the delineation between acquisition and TTP. There is clear evidence of this from Figure 2 at the top of the pyramid where it lists “Tools and TTP.” The bottom line is acquisitions and TTP are not the same and they need to be treated so. In the case of the military; tactics define “why” you employ your weapon system in a specific manner. The cyber tactics example that is used in the AFSPCI 11-260 is re-configuring a network in response to a network intrusion threat. The tactic is the network protection re-configuration. The cyber techniques are ways or methods used to perform missions, functions, or tasks. An example of this is defending a network through layered defenses including filter, proxies, and/or sensors at multiple levels across the network infrastructure to prevent unauthorized access to network resources to access or disrupt information. The last part of TTP is procedures which are standard, detailed steps that prescribe how to perform specific tasks. Think of the procedure as a check list and/or standard operating procedure. It is the TTP that have been proven to change rapidly; not the acquisition. In reality the underlying technology that the cyber continuum operates in is based off of request for comments that have been around for decades.

Many of the cyber related discussions that have been in the news today are about issues in security due to vulnerabilities in the software. The exploitation of the vulnerabilities coincides with TTP to affect the hardware and/or software. Few examples, buffer over flows, worms, viruses, denial of service, and phishing emails are methodologies to exploit a system. These should not be confused with a new technology; they are TTP. Therefore the perceived need for “rapid” cyber acquisitions could be derived from the misconception that operations, like email or the Internet, are in use at demand and there needs to be an acquisition in place to move at that same high paced rate. However, just because someone is able to send an email to the other side of the world within a matter of seconds, should not mean that the acquisition process must match that pace.

TTP is gleamed every day through venues such as exercises, training vignettes, conferences, briefings and contingencies operations. Some of the organizations that are tasked to facilitate these lessons learned are underutilized and under staffed. Many times the cost of creating TTP is unbelievably small in contrast to system acquisition.

The cyber domain has taken a approach that is somewhat different than air and space in regards to TTP development with the creation of the TDI methodology. The TDI process has proven beneficial for the cyber community because it is a unique avenue to validate and document the rapidly evolving cyberspace domain [36].

5.1.4 Overall Assessment

The current paradigm is still unresolved at this time due to the fact that there is so much fluxuation within the cyber acquisition community. A major turning point in cyber acquisitions are the solutions that are being discussed that answer the NDAA. If approved and put into law, there will be a clear delineation between two cyber acquisition frameworks. These two processes, rapid and deliberate, are intended to accommodate the pace and speed of cyberspace operations and to cover the full range of development approaches. The processes are designed as templates to place requirements, development, testing, and oversight into the nominal frames of the traditional acquisition process. Both processes incorporate cross-cutting enablers such as system engineering, technology insertion, collaboration services, and capability repositories.

If the rapid scenario, like described in the NDAA, is warranted then the most likely scenario for the process to be successful is for the program to already be under development or in existence in the commercial sector (e.g. COTS and GOTS). That would also mean a close collaboration with the cyber commercial industry. The commercial industry is an invaluable resource to indentify cyber threats and vulnerabilities, and posses' expertise to advise the DoD on technical standards and solutions to military requirements.

5.2 Organizations

5.2.1 AFOTEC

If AFOTEC is going to start testing large cyber PoR, such as CITS, then they need to have proper manning of cyber SMEs. DoD is currently revamping its organizations to find ways to minimize financial costs and one of the main ways to resolve this is reducing or combining organizations. If the DoD is going to strategically develop a new command with the prime mission of planning, coordinating, integrating, synchronizing, and directing activities to operate and defend the DoD information networks, then it would seem unwise to not have an internal organization within themselves to properly handle the mission. If this is not done, then the DoD is going to be creating a shell of an organization which will not be able to successfully augment their mission within the cyber arena.

Another conundrum that AFOTEC needs to consider is if they stand up a detachment that has the sole mission for cyber testing then they will need to properly staff them not only with cyber experts but also individuals that have knowledge within the acquisitions and test arena.

5.2.2 ALSA

Even though the focus of the paper concentrated on AF cyber initiative there are many ways to co-develop the cyber domain. The MTTP is a way to get all the Services on a concurrent vector and will augment means to learn from each other's capabilities.

ALSA's MTTP will not be rapidly evolving as fast as AFTTP since MTTP are revised every two to three years. They also must be approved by the joint actions steering group which consists of the four-Services at the General Officer and Senior Executive Staff level. The mission of ALSA states they will "rapidly and responsively develop MTTP" but their cyclic process lags behind the process that generates AFTTP.

5.2.3 JT&E

As previously stated the AF's conduit into the JPO, which is the facilitator for submitting the nominations of JT and QRTs, is the AFJO. AFOTEC use to be the conduit into the JPO but the responsibilities was divided between the two organizations. AFJO provide continuous, proactive management of AF participation in the OSD JT&E Program.

AFJO would be the organization to help develop any cyber JT and/or QRT submissio from AFSPC. The outcome of the JT&E will be solutions to solve multi-service operational problems in a joint environment and alleviate T&E difficulties through work on testing methodologies. It is up to ALSA and the JPO/AFJO if they will reside within ALSA documentation or if there is another means to disseminate the information in a more productive means. Another means to disseminate the lessons learned is the stand up of a new organization that's mission would be to resolve the deficiency for the test submission. Usually, the JT would be the type of test that would warrant this type of activity. An example would be the stand up of the joint digital integration for combat engagement (JDICE). JDICE was originally stood up from a JT due to the lack timely, accurate, actionable, and tactically significant data to current and future platforms. JDICE's mission is to facilitate innovative, near-term solutions to C2ISR and contributes to modernization planning, resource prioritization, and configuration control--transcending all areas of joint and coalition operations [14].

The lessons learned that are derived from the joint testing will augment other types of documentation from joint doctrine to multi-service doctrine. The main difference between the two doctrines is joint doctrine is operational level doctrine and multi-service doctrine are the tactical level solutions.

5.3 Cyber Venues

Most people know the analogy that "practice makes perfect." This no doubt holds even truer in the cyber world. One way to in increase the effectiveness of the cyberspace domain is to work together as a united entity. One place the cyber warriors will get that practice is at the Red Flag exercise that is held multiple times a year at Nellis AFB, Nevada. There are other training exercises besides Red Flag that have a more cyber focus but Red Flag intersects the air, space and cyber domains [30].

The Red Flag exercise is a realistic combat training exercise that involves training AF operators and its allies in simulated air/space/cyber combat on the NTTR. The exercise was born in the post-Vietnam era to improve combat performance by closely simulating wartime scenarios and quickly became ACC's premier tactical air training exercise, providing mission ready crews the most realistic training environment possible, outside of real operations. The life expectancy of American pilots during the operations in Vietnam increased dramatically after ten combat missions. Red Flag gave pilots, crews and support agencies the chance to train realistically in combat situations -- thus increasing their chance of survival within the first ten days of any combat operation [31]. Cyber and space operators have been involved in Red Flag for the past six years but many of the vignettes within the exercise were "white carded"; meaning they were simulated. Just this past year the organizers of the Red Flag exercise have included the cyber operators but without the "white card" effect. The exercise will inundate cyber operators with inputs to push them to the limit of their expertise. Many have said the first year was a high learning curve for the cyber operators but feel this will be the premier event to work with their brethren in the air and space domains [30].

Unlike the air and space domain once the infrastructure is established there will be minimal future costs for integration into the Red Flag venue. There are large cost associated with the air domain due to the fact they bring in the majority of their aircraft from out of state and sometime out of country.

Another point of discussion is the new weapons instructor course (WIC) that is also being held at Nellis. Two times a year a cadre of SMEs will train the next generation of cyber warriors.

The history of the weapons school's origins date back to 1949, when it began as the Aircraft Gunnery School, through 1987, the school focused on training fighter pilots; it now trains Airmen in bombers, cargo aircraft, unmanned aerial systems, intelligence, space and more. The weapons school, known as the U.S. Air Force Fighter Weapons School from 1954-1992, began transitioning from an exclusively fighter pilot program in the 1980s. In 1986, the school activated the air weapons controller division, later known as the C2 operations division. The school gained a fighter intelligence officers course in 1988, which became the graduate patch-awarding intelligence division in 1990. The school continued to expand in the 21st century, with the Air Force's growing need for weapons officers skilled at integrating all aspects of air, space and cyber power. Special operations forces also became part of the weapons school in 2000, developing courses for the MH-53 and AC-130 [31]. The new addition is a huge turning point for understanding what their expertise can add to the other domains.

5.4 Discussion

This research set out to identify if there is a need for rapid cyber acquisitions in the AF. The findings imply that the current paradigm for rapid cyber acquisitions is insufficient. Indeed, the current construct is more aptly designed around large-scale, significant programs similar to air and space processes. Interestingly, however, upon further analysis, the research determined that there has yet to be a requirement set forth identifying a capability need to be addressed via a rapid acquisition process. Rather, all identified rapid capability requirements were successfully addressed via TTP and operational solutions. Indeed, this research was unable to reveal a situation in which the lack of a rapid acquisition process prevented the delivery of a cyber capability as required.

The implication of this notion is that TTP are more adept at fulfilling rapid capability requirements than the acquisition construct. For example, CITS block 30 provides the necessary infrastructure and aligns with a traditional acquisition asset. However, configuration and manipulation to prevent or thwart malicious actions is a real-time function associated with TTP. In essence, the day-to-day network warfare operations are enabled by existing capabilities and rapid implementation of tactics—all aspects readily addressed using non-material solutions. Additionally, configuration and maintenance of network actions do not require a rapid acquisition process. For example, updating virus signatures is an O&M/sustainment function and not a requirement that aligns with traditional acquisition, such as an airframe block update.

VI. Conclusions and Recommendations

6.1 Conclusions

The research in this report clearly identifies a growth in the creation and development of AFTTP. The evidence clearly states there needs to be a continued effort of support to this rapid TTP process. The 561 JTS is the only organization tasked with the facilitation of AFTTP. The discussion that cyberspace is an equal war fighting domain implies that the squadron should be manned with an adequate number of cyber SMEs. Note that there is a SME for every MA and aircraft (or aircraft category) but only one cyber representative for the cyber domain.

AFOTEC lists cyber as part of Detachment 4's mission located at Paterson AFB, Colorado. When contacted, the SMEs within cyber and T&E agreed that having a detachment in San Antonio would prove beneficial because AFOTEC has been requesting assistance from the 346 TS. Standing up a specific detachment with a centralized focus on cyber testing would help the community immensely. The creation of the cyber detachment must also come with money and experienced personnel. The major key to this standup is to minimize the workload of the 346 TS.

In the wake of the 9/11 attacks, representatives from North American Aerospace Defense Command (NORAD) and Central Region NORAD (CONR) convened a conference to derive the lessons learned. Their solution was the development and creation of an MTTP called Air Defense of the U.S. (ADUS). The MTTP solidified best practices and lessons learned from what came out of the horrific tragedy [34]. This is something that needs to be done today for cyber. Not only is it important to unite the cyber warriors through MTTP and joint documentation but there's a strong need to harness the wartime lessons learned.

6.2 Recommendations

Chapter 5 concluded that the current cyber acquisitions paradigm for rapid cyber acquisitions is insufficient. That conclusion is based on the fact, to date; there have not been any programs that have met a rapid acquisition timeline. In spite of that fact, there are already methods in place for supplying the metamorphosing cyber capabilities through the delivery of TTP to the cyber community. The overall recommendation is the need to increase awareness and educate the cyber community of these options and methods of solving cyber requirements through non-material solution TTP.

The following five items are propositions to conclude the overall recommendation:

1. Increase cyber SME manning at the tactical level squadrons that have direct impact of AFTTP
2. AFSPC should submit more cyber issues with submission of JT and QRTs through AFJO
3. Create an AFOTEC detachment that has a primary mission of OT&E within the cyber domain
4. ALSA should sponsor the creation of a cyber MTTP
5. Continue the sponsorship and development of the cyber SMEs within venues like Red Flag and a cyber WIC through proper manning and financing

The research recommendation is to increase the manning of organizations with primary missions that create development and facilitate AFTTP. The research also suggests that the AFTTP within cyber not only have increased in the total number per year but also shown to outpace the number of reports compared to the air and space domains. This again seems contradictory to the number of cyber SMEs within organizations that support AFTTP.

The research recommendation is to continue to educate and submit areas of focus that may be lacking in the cyber domain through rigorous JT&E. The submission of QRTs would be a quicker way to find solutions to the problem due to the fact that QRTs last only one year. If there seems to be a larger issue in the cyber domain that needs more attention, then a submission of a JT would be in order. The JT would need to be approved through a nomination process that lasts a year, while the JT would last three years. With that being said, it would be four years until the JT&E report would be signed and vetted to the cyber community.

The research recommendation is there is a need to create a new AFOTEC detachment that is focused on the cyber OT&E mission. The location that would be most beneficial is San Antonio where the 46 TS who conducts the developmental testing and the 346 TS who conducts the OT&E. These two squadrons have a combined test force construct already in place to augment a more streamlined testing process. Also, by standing up an AFOTEC detachment in San Antonio would leverage different backgrounds of personnel within the combined test force (e.g. 46 TS and 346 TS).

The research recommendation due to the fact that there is not a cyber MTTP is to develop one in the near future. The MTTP would augment USCYBERCOM which is multi-service. These MTTP would increase the likelihood of getting all the services on a concurrent vector within the cyber community.

The AF has a series of unclassified and classified documents called AFTTP 3-3 and AFTTP 3-1 that are specific to the weapons system and/or MA. For example, there is documentation for each specific fighter, bomber, and space platform. The AF currently has an AFTTP 3-1 in the final stages of approval. This AFTTP 3-1 would be to be a helpful template for the creation of a MTTP to help indentify TTP methods used within the other Services.

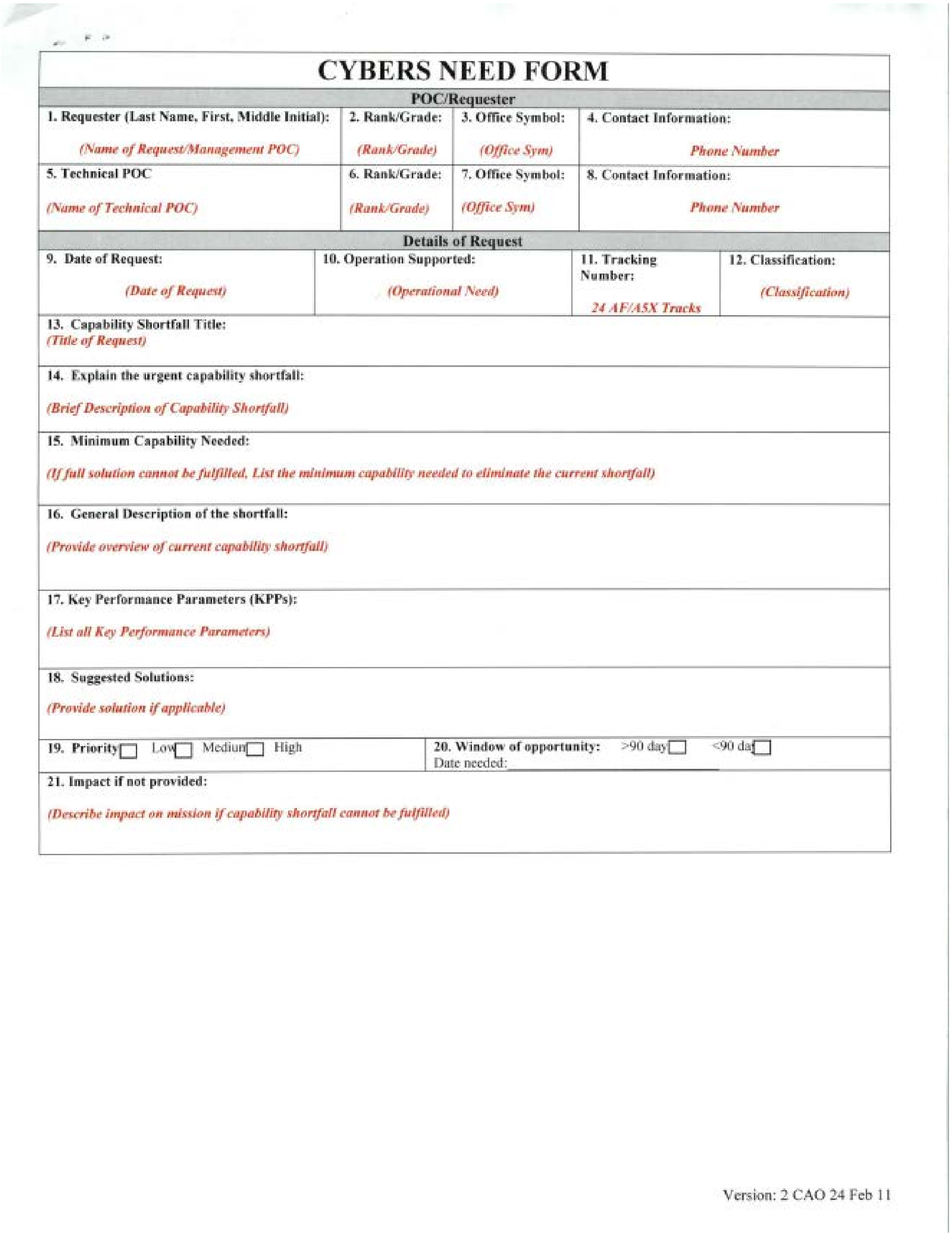
The research recommendation is to continue to involve the cyber experts within exercises that will solidify AFTTP. One prime is example is the Red Flag exercise for incorporating kinetic and non-kinetic vignettes. Another great achievement within the cyber community was the stand up of a weapon school flight contained within the 328 Weapons Squadron at Nellis AFB, Nevada. The stand up of the weapons school squadron will increase awareness and enhance visibility of cyber to the rest of the AF.

6.3 Future Considerations

This research paper only touched upon a small fraction of the acquisition cycle and how it relates to cyber. Figure 1 shows a complex architecture. This research primarily focused on the right hand side of the graphic in Figure 1. Future research should consider examining other sections of the acquisition cycle, for example, requirements development, R&D and financial considerations which would be on the left to middle portions of the graphic in Figure 1. A major trend in the research showed that defining capabilities and requirements within the cyber domain has proven difficult largely due to the fact that cyber is not always a tangle item, as opposed to, an aircraft or a satellite. With that said, it makes it difficult to submit financial requests for cyber because the requirements and capabilities are not well defined. An example approach for research is the systems engineering approach to see if there are quicker means to alleviate the process in Figures 4 and 5. For example, if capabilities are purchased through a commercial contractor (e.g. COTS/GOTS) there may not be a need to proceed through milestones A-C; there may be a way to combine all three or combine A and B then later transition to C. Either approach would have its advantage and disadvantage but the goal is for continual improvement in the acquisition system.

Appendix A

Cyber Needs Form – Dated 24 Feb 2011



CYBERS NEED FORM

POC/Requester

1. Requester (Last Name, First, Middle Initial): *(Name of Request/Management POC)*	**2. Rank/Grade:** *(Rank/Grade)*	**3. Office Symbol:** *(Office Sym)*	**4. Contact Information:** *Phone Number*
5. Technical POC *(Name of Technical POC)*	**6. Rank/Grade:** *(Rank/Grade)*	**7. Office Symbol:** *(Office Sym)*	**8. Contact Information:** *Phone Number*

Details of Request

9. Date of Request: *(Date of Request)*	**10. Operation Supported:** *(Operational Need)*	**11. Tracking Number:** *24 AF/A5X Tracks*	**12. Classification:** *(Classification)*

13. Capability Shortfall Title:
(Title of Request)

14. Explain the urgent capability shortfall:

(Brief Description of Capability Shortfall)

15. Minimum Capability Needed:

(If full solution cannot be fulfilled, List the minimum capability needed to eliminate the current shortfall)

16. General Description of the shortfall:

(Provide overview of current capability shortfall)

17. Key Performance Parameters (KPPs):

(List all Key Performance Parameters)

18. Suggested Solutions:

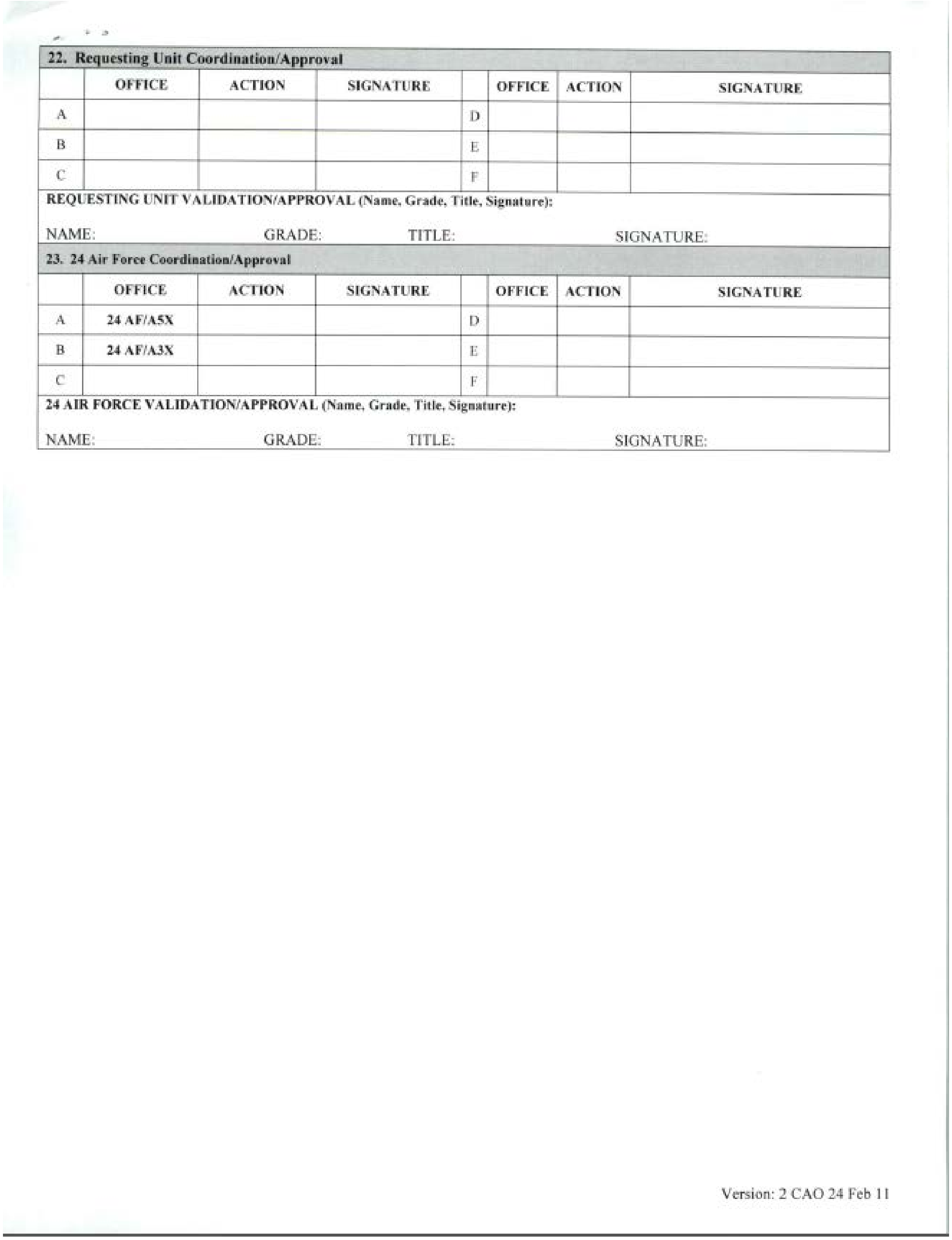
(Provide solution if applicable)

19. Priority□ Low□ Medium□ High	**20. Window of opportunity:** >90 day□ <90 da□ Date needed:________________

21. Impact if not provided:

(Describe impact on mission if capability shortfall cannot be fulfilled)

Version: 2 CAO 24 Feb 11



22. Requesting Unit Coordination/Approval

	OFFICE	ACTION	SIGNATURE		OFFICE	ACTION	SIGNATURE
A				D			
B				E			
C				F			

REQUESTING UNIT VALIDATION/APPROVAL (Name, Grade, Title, Signature):

NAME: GRADE: TITLE: SIGNATURE:

23. 24 Air Force Coordination/Approval

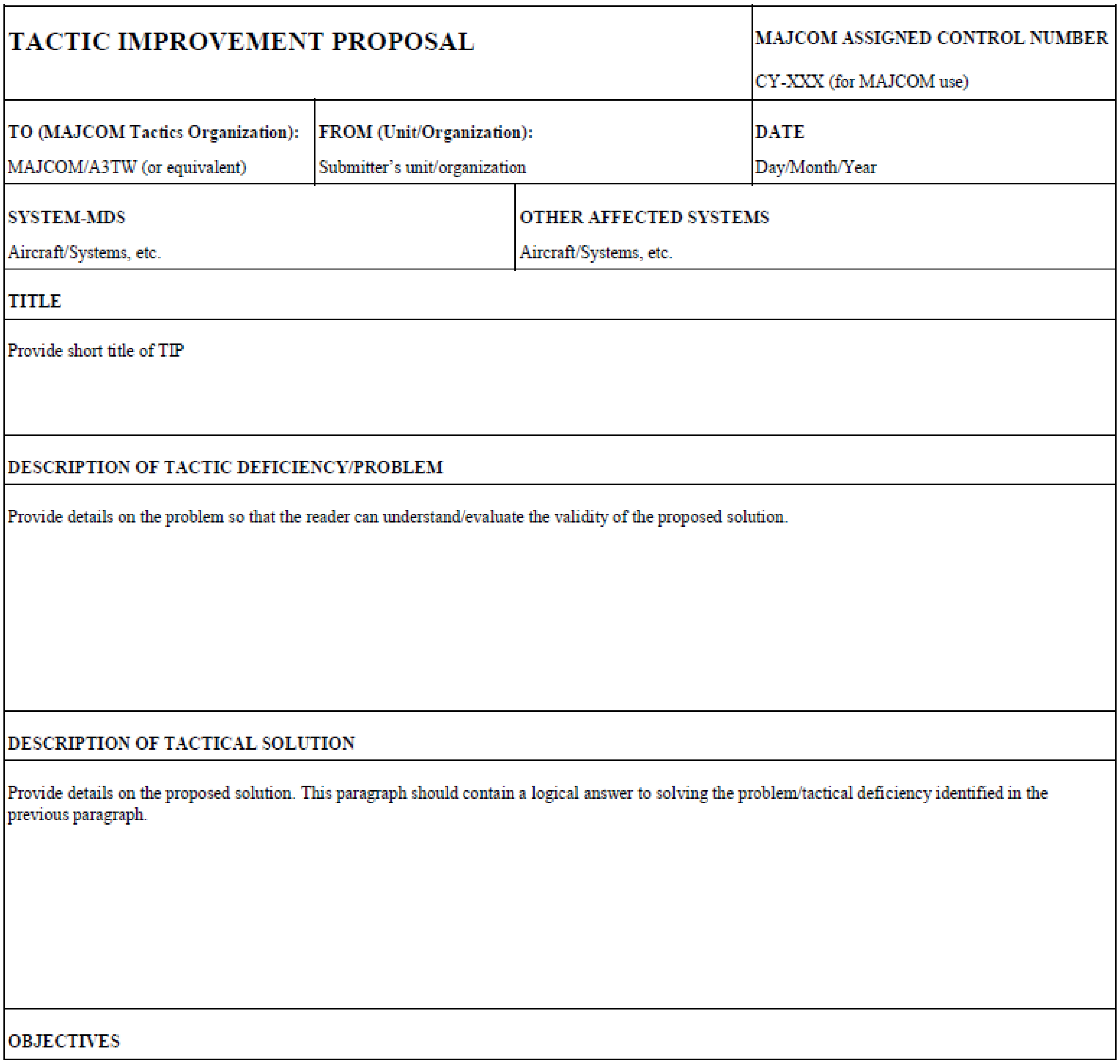
	OFFICE	ACTION	SIGNATURE		OFFICE	ACTION	SIGNATURE
A	**24 AF/A5X**			D			
B	**24 AF/A3X**			E			
C				F			

24 AIR FORCE VALIDATION/APPROVAL (Name, Grade, Title, Signature):

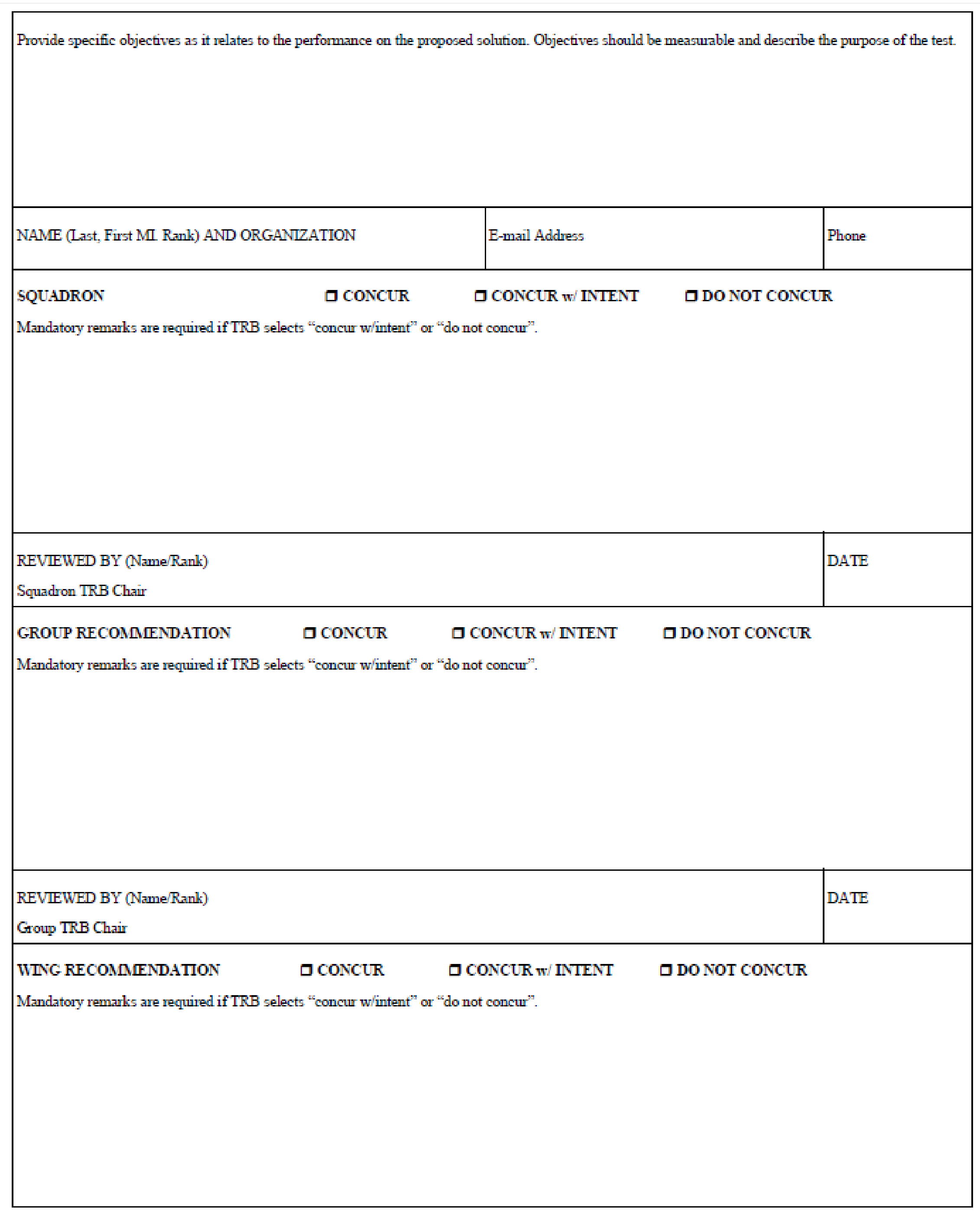
NAME: GRADE: TITLE: SIGNATURE:

Appendix B

AF Form 4326 - Tactics Improvement Proposal – Dated 29 Sept 2011



TACTIC IMPROVEMENT PROPOSAL		**MAJCOM ASSIGNED CONTROL NUMBER** CY-XXX (for MAJCOM use)
TO (MAJCOM Tactics Organization): MAJCOM/A3TW (or equivalent)	**FROM (Unit/Organization):** Submitter's unit/organization	**DATE** Day/Month/Year
SYSTEM-MDS Aircraft/Systems, etc.	**OTHER AFFECTED SYSTEMS** Aircraft/Systems, etc.	
TITLE		
Provide short title of TIP		
DESCRIPTION OF TACTIC DEFICIENCY/PROBLEM		
Provide details on the problem so that the reader can understand/evaluate the validity of the proposed solution.		
DESCRIPTION OF TACTICAL SOLUTION		
Provide details on the proposed solution. This paragraph should contain a logical answer to solving the problem/tactical deficiency identified in the previous paragraph.		
OBJECTIVES		



Provide specific objectives as it relates to the performance on the proposed solution. Objectives should be measurable and describe the purpose of the test.

NAME (Last, First MI. Rank) AND ORGANIZATION	E-mail Address	Phone

SQUADRON ❐ **CONCUR** ❐ **CONCUR w/ INTENT** ❐ **DO NOT CONCUR**

Mandatory remarks are required if TRB selects “concur w/intent” or “do not concur”.

REVIEWED BY (Name/Rank) Squadron TRB Chair	DATE

GROUP RECOMMENDATION ❐ **CONCUR** ❐ **CONCUR w/ INTENT** ❐ **DO NOT CONCUR**

Mandatory remarks are required if TRB selects “concur w/intent” or “do not concur”.

REVIEWED BY (Name/Rank) Group TRB Chair	DATE

WING RECOMMENDATION ❐ **CONCUR** ❐ **CONCUR w/ INTENT** ❐ **DO NOT CONCUR**

Mandatory remarks are required if TRB selects “concur w/intent” or “do not concur”.

REVIEWED BY (Name/Rank) Wing TRB Chair	DATE
MAJCOM/NAF RECOMMENDATION **□ CONCUR** **□ CONCUR w/ INTENT** **□ DO NOT CONCUR** Mandatory remarks are required if TRB selects "concur w/intent" or "do not concur".	
REVIEWED BY (Name/Rank) MAJCOM/NAF TRB Chair	DATE
AFSOF/MAF RECOMMENDATION **□ CONCUR** **□ CONCUR w/ INTENT** **□ DO NOT CONCUR** **□ N/A** Mandatory remarks are required if TRB selects "concur w/intent" or "do not concur". N/A will be used when a TIP is deemed CAF-related and therefore is not routed through the AFSOF/MAF TRB.	
REVIEWED BY (Name/Rank) AFSOF/MAF Working Group Chair	DATE
CAF TRB ACTION **□ CONCUR** **□ CONCUR w/ INTENT** **□ DO NOT CONCUR** **□ N/A** Mandatory remarks are required if TRB selects "concur w/intent" or "do not concur". N/A will be used when a TIP is deemed AFSOF or MAF-related and is not routed through the CAF TRB.	
REVIEWED BY (Name/Rank) CAF Working Group Chair	DATE

Appendix C

Point of Contacts for this Research

346 Test Squadron
AFSPC/A3TW
AFOTEC/A-8
AFOTEC/Cyber Test Division
AFSPC/A3T
AFSPC SIDC/595
46 Test Wing
AFSPC/A5JI
AFSPC/A3TO
AFSPC/A5J
SAF/AQR
AFMC/A2
AFSPC/A3ID
605 TES
90 IOS
AFMC/A5PM
ESC/XR3
26 OSS
DoD CIO/Acquisition Directorate
561 JTS
Air Force TENCAP
8 WPS
46 Test Squadron
AFSPC/A3I
645 ALSG
AF/A3Z-CI
IO Directorate, OUSD(P) DASD SO/LIC CT
505 Command and Control Wing
Directorate for IO, ODASD (SO&CT)
USAF Warfare Center
57 WG
Big Safari Program Office
328 WPS
Air Force Joint Test and Evaluation Office (AFJO)
Joint Program Office
ACC/A3TW
AF/A2
Air Land Sea Application (ASLA) Center
Aeronautical System Center

Appendix D
Acronyms with the Terms and Definitions

Operational Suitability (OS) – The degree to which a system can be placed satisfactorily in field use with consideration given to availability, compatibility, transportability, interoperability, reliability, wartime usage rates, maintainability, safety, human factors, manpower supportability, logistics supportability, natural environmental effects and impacts, documentation, and training requirements.

Operational Effectiveness (OE) – The overall degree of mission accomplishment of a system when used by representative personnel in the environment planned or expected (e.g., natural, electronic, threat) for operational employment of the system considering organization, doctrine, tactics, survivability, vulnerability, and threat (including countermeasures, initial nuclear weapons effects, and nuclear, biological, and chemical (NBC) contamination threats).

Verification, Validation and Accreditation (VV&A) – (1) Verification: The process of determining that a model or simulation (or other test capability) implementation accurately represents the developer‘s conceptual description and specifications. For model and simulation, verification also evaluates the extent to which the model and simulation has been developed using sound and established software-engineering techniques. (2) Validation: The process of determining (a) the manner and degree to which a model and simulation (or other test capability) is an accurate representation of the real-world from the perspective of the intended uses of the model and simulation, and (b) the confidence that should be placed on the assessment. (3) Accreditation: An official determination that a model or simulation is acceptable for a specific purpose, and is based on a five-step process: identify test issues; review validation documentation; compare test capabilities and validation information with test issues; identify potential shortfalls; and develop and execute strategy to address shortfalls (assess risk).

Operational Utility Evaluation (OUE) – Are evaluations conducted to demonstrate or validate new operational concepts or capabilities, upgrade components, or expand the mission or capabilities of existing or modified systems. OUEs are not used when IOT&E, QOT&E, or FDE are required or are more suitable.

Advanced Concept Technology Demonstration (ACTD) and Joint Capability Technology Demonstration (JCTD) – Serve to accelerate and facilitate the application of mature advanced technologies to provide near-term solutions to meet joint requirements.

Military Utility Assessment (MUA) – An assessment of operational utility completed at the end of an ACTD/JCTD.

Initial Operational Test and Evaluation (IOT&E) – An independent and dedicated operational T&E conducted in as realistic an operational environment as possible to estimate the prospective system's overall operational capability determined by effectiveness, suitability, and other operational considerations. In addition, OT&E provides information on organization, personnel requirements, doctrine, and tactics. It may also provide data to support or verify material in operating instructions, publications, and handbooks.

Multiservice Operational Test and Evaluation (MOT&E) – OT&E conducted by two or more services on systems to be acquired by more than one service or to be interoperable between services.

Follow–on Operational Test & Evaluation (FOT&E) – Continuation of IOT&E or QOT&E. FOT&E answers specific questions about unresolved COIs and test issues, verifies the resolution of deficiencies determined to have substantial or severe impact on mission operations, or completes areas not finished during the I/QOT&E. Requirements for FOT&E are documented in an approved AFOTEC OT&E report prior to the planning of the FOT&E.

Qualification Operational Test and Evaluation (QOT&E) – The operational testing performed on programs instead of IOT&E for which there is no RDT&E-funded development effort.

Joint Test and Evaluation (JT&E) – JT&E candidate programs are nominated by the Services, and directed and funded by OSD. JT&E programs evaluate technical or operational concepts that are applicable to more than one Service. They usually do not result in the acquisition of systems.

Initial Test Design (ITD) – Initial test design is another focus of Early Influence. It is a systematic approach to take the test teams from capability requirements to credible OT&E constructs which, when executed, will yield the final data required by decision-makers to make program decisions. ITD is a process to provide a standardized approach for the corporate allocation of resources among all of the test programs managed by AFOTEC and to identify major test capability requirements and shortfalls.

The following terms provide definitions and explanations of operational testing and are ordered in the sequence of program or system maturity.

Early Operational Assessment (EOA) – Conducted to provide insight into progress being made toward operational effectiveness, suitability, and mission capability. The OT&E construct will form the basis for the early operational assessment. The construct used for the EOA may not be the final construct, but it should give insight into the elements that make up effectiveness and suitability for the system under test. EOAs also look into the program‘s future based on current information and observations to assess readiness for OT&E.

Operational Assessment (OA) – Analysis of progress toward operational effectiveness and suitability made by an independent operational test activity, with user support as required, on other than production systems. Additionally, AFOTEC assess progress toward overall mission capability. The focus of an operational assessment is on significant trends noted in development efforts, programmatic voids, areas of risk, adequacy of requirements, and the ability of the program to support adequate operational testing. Operational assessments may be made at any time using technology demonstrators, prototypes, mockups, engineering development models, or simulations, but are substitute for the independent OT&E necessary to support full production decisions. An OA conducted before MS B is referred to as an EOA.

Operational Utility Assessment (OUA) – are used to determine operational utility in support of assessments conducted on innovation programs. An OUA is planned, conducted, and reported by adapting the OT&E construct to the technology being assessed.

Bibliography

1. Garstka, John and Leyva, Gabe. “Acquiring Cyber Capabilities Framework” brief. Department of Defense CIO office. 13 September 2011.

2. Butler, Amy. “Welcome to the Jungle: Big Safari for Cyberspace”. Aviation Week. 12 April 2010. http://www.aviationweek.com/aw/blogs/space/index.jsp?plckController=Blog&plckScript=blogScript&plckElementId=blogDest&plckBlogPage=BlogViewPost&plckPostId=Blog%3A04ce340e-4b63-4d23-9695-d49ab661f385Post%3Ae4f0118b-b239-4036-a4c7-0b2612f0bf7d

3. Department of Defense. Department of Defense Directive 5000.1. Washington: GPO. Certified current as 20 November 2007. http://www.dtic.mil/whs/directives/corres/pdf/500001p.pdf

4. Department of the Air Force. Air Force Doctrine Document. Cyberspace Operations 3-12. Washington: HQ USAF, 15 July 2010. http://www.govexec.com/features/0811-15/0811-15mag.htm

5. Butler, Matt Major. “Acquisition & Test of Cyberspace Operations”. CSCE 525 Paper. Air Force Institute of Technology. Summer 2011.

6. Tirpak, John. “Operational Acquisition”. Air Force Magazine. Vol. 87, No.8 August 2004. http://www.airforcemagazine.com/MagazineArchive/Pages/2004/August%202004/0804operation.aspx

7. Department of Defense. Office of Secretary of Defense. Washington: GPO. certified current as 9 April 2009. https://www.mpm.osd.mil/documents/OUID051606_IACategory.pdf

8. Department of Defense. Department of Defense Directive. DoDI 5000.2 Washington: GPO. 8 December 2008. http://www.dtic.mil/whs/directives/corres/pdf/500002p.pdf

9. Buaxbaum, Pater A. “Building a Better Cyber Range”. International Relations and Security Network. 2 August 2011. http://www.isn.ethz.ch/isn/Current-Affairs/ISN-Insights/Detail?lng=en&id=131577&contextid734=131577&contextid735=127714&tabid=127714&dynrel=4888caa0-b3db-1461-98b9-e20e7b9c13d4

10. A Brief History and Heritage of AFOTEC. 24 October 2011. http://www.afotec.af.mil/shared/media/document/AFD-111024-020.pdf

11. AFOTEC Program Manger Tool Kit, Dated, 3 October 2011. http://www.afotec.af.mil/shared/media/document/AFD-111020-027.pdf

12. Fischer-Carter, Tamerara "AFSPC Commander Addresses Maturing Cyberspace Domain". Air Force Print News. 2 February 2012. http://www.af.mil/news/story_print.asp?id+123290240

13. C. Todd Lopez, SSgt, "8th Air Force to Become New Cyber Command". Air Force Online News. United States Air Force. 3 November 2006. http://www.af.mil/news/story.asp?storyID+123030505

14. "JDICE: A Common Picture for TAC-Air Controllers". Defense Industry News. 28 March 2007. http://www.defenseindustrydaily.com/jdice-a-common-picture-for-tacair-controllers-03173/

15. White, Ed. "Air Force TENCAP Celebrates Three Decades of Impressive Warfigthter Support Programs". Air Force Print News Today. United States Air Force. 26 August 2008. http://www.afspc.af.mil/news1/story.asp?id=123112413

16. McNabb, Scott, TSgt. "346th Test Squadron Practices the 'Art' of Cyber Testing". Air Force Online News. United States Air Force. 30 November 2011. http://www.24af.af.mil/news/story.asp/id=1323281668

17. Gertz, Bill. "Inside the Ring: Cyberwarfare Acquisition". The Washington Times. 8 February 2012. http://www.washingtontimes.com/nes/2012/feb/8/inside-the-ring-776061934

18. Washington Business Journal. "Air Force Cyber Chief: Speed up Acquisitions". 9 February 2012. http://www.bizjournals.com/washington/blog/fedbiz/daily/2012/02/air-force-cybercief-speed-up.html

19. Air Force Instruction 10-602. Determining Mission Capability and Supportability Requirements. Washington: HQ USAF. 18 March 2005. www.e-publishing.af.mil/shared/media/epubs/AFI10-602.pdf

20. Air Force Instruction 10-602. Acquisition and Sustainment Life Cycle Management. Washington: HQ USAF. 8 April 2009. www.e-publishing.af.mil/shared/media/epubs/AFI63-101.pdf

21. Air Force Instruction 99-103. Capabilities-Based Test and Evaluation. Washington: HQ USAF. 20 March 2009. www.e-publishing.af.mil/shared/media/epubs/AFI99-103.pdf

22. Air Force Instruction 11-260. Tactics Development Program. Washington: HQ USAF. 15 September 2011. www.e-publishing.af.mil/shared/media/epubs/AFI11-260.pdf

23. McVay, Justin Capt. “Nellis Activates New Joint Tactics Unit”. Air Force Print News. 25 October 2006. http://www.nellis.af.mil/news/story.asp?id=12302996

24. Crisp M.D. Directive for the Joint Threat Assessment and Negation for installation infrastructure control systems Quick Reaction Test. Office of the Secretary of Defense. 4 Jan 2012. http://www.jte.osd.mil/jtecurrentprojects.asp

25. Crisp M.D. Directive for the Joint Cyber Operations Joint Test. Office of the Secretary of Defense. 4 Aug 2010. http://www.jte.osd.mil/jtecurrentprojects.asp

26. Hayden, Michael General. “The Future of Things Cyber”. Strategic Studies Quarterly. Spring 2011. http://www.au.af.mil/au/ssq/2011/spring/hayden.pdf

27. McCullough, Amy. “Cyber Futures”. Air Force Magazine. 26 March 2012. http://www.airforce-magazine.com/MagazineArchive/Pages/2011/June%202011/0611cyber.aspx

28. Nakashima, Ellen. “More Clout Sought For Military’s Cyber Warfare Unit”. Washington Post. 2 May 2012. http://www.washingtonpost.com/world/national-security/military-officials-push-to-elevate-cyber-unit-to-full-combatant-command-status/2012/05/01/gIQAUud1uT_story.html

29. Herman, Arthur. “The Pentagon vs. Defense”. New York Post. 6 May 2012. http://www.nypost.com/p/news/opinion/opedcolumnists/the_pentagon_vs_defense_7nMIKp97MSz1pOzHYTh2eN

30. McNabb, Scott, TSgt. “Red Flag Cyber Operations: Part I – Isn’t Red Flag a Flyer’s Exercise?”. Air Force News. 3 February 2011. http://www.nellis.af.mil/news/story.asp?id=123244822

31. Richard, Jennifer 2Lt. “New Patch Reflects Weapons School’s Expansion, New Courses”. Air Force News. 1 February 2009. http://www.nellis.af.mil/news/story.asp?storyID=123130004

32. "AFOTEC Commander Inactivates Detachment 3". Air Force News. 4 April 2010. http://www.afotec.af.mil/news/story.asp?id=123199043

33. Library of Congress. January 2012. http://thomas.loc.gov/cgi-bin/query/F?c111:1:./temp/~c111gtaYxa:e496844:

34. Finn, Robert Jr. "It's Time to Redouble Efforts in Multiservice TTP". Armed Forces Journal. April 2012. http://www.armedforcesjournal.com/2012/04/9772614

35. Air Force Instruction 99-106. Joint Test and Evaluation Program. Washington: HQ USAF. 26 August 2009. http://www.e-publishing.af.mil/shared/media/epubs/AFI99-106.pdf

36. Air Force Space Instruction 11-260 Tactics Development Program. 29 November 2011. http://www.e-publishing.af.mil/shared/media/epubs/AFSPCI10-260.pdf

37. Paone, Chuck. "Net-centricity Transcends the Network". Air Force Material Command. 66th Air Base Group Public Affairs. 22 October 20010. http://www.afmc.af.mil/news/story.asp?id=123223090

38. DoD Strategy for Operating in Cyberspace. Department of Defense. July 2011. http://www.defense.gov/news/d20110714cyber.pdf

39. Haywood, James, Brig. Gen. Brief at the 2011 AFA Space and Cyberspace Warfare Symposium. 17 November 2011. http://www.spacewarfare.org/ASSETS/Briefings%202010/2%20Haywood%20A5%20Keystone%20Charts.pptx

40. Air Force Instruction 63-144. Quick Reaction Capability Process. Washington: HQ USAF. 4 January 2011. http://www.e-publishing.af.mil/shared/media/epubs/AFI63-114.pdf

41. Air Land Sea Application Center. Organizational Brief. April 2012. http://www.jte.osd.mil/jtecurrentprojects.asp

42. Thompson, David, Brig. Gen. AFSPCGM63-1. "AFSPC Guidance Memorandum on Real-Time Operations and Innovation." 27 October 2011.

Vita

Major Matt J. Butler graduated from Eden Prairie High School in Eden Prairie, Minnesota. He entered undergraduate studies at Augsburg College in Minneapolis, Minnesota where he graduated with a Bachelor of Science in Physics in 1998. He was commissioned through the AFROTC Detachments 410 at the University of St. Thomas where he was nominated for a Regular Commission.

Major Butler's prior assignments include working at a Command and Reporting Center (CRC), flying on the E-8C Joint Surveillance Target Attack Radar System (Joint STARS), and an operations officer at a test and evaluation squadron. In May 2011, he started his intermediate development education at the Air Force Institute of Technology. Upon graduation, he will be assigned to Air Combat Command within the Plans, Programs, and Strategy division at Langley AFB, Virginia.

Major Butler is a senior air battle manager with over 1,100 flying hours in JSTARS. He has served in Operations Northern Watch, Joint Forge, Enduring Freedom, Noble Eagle and Iraqi Freedom.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)* 14-06-2012	**2. REPORT TYPE** Graduate Research Paper	**3. DATES COVERED** *(From – To)* June 2011 – June 2012

4. TITLE AND SUBTITLE

Rapid Delivery of Cyber Capabilities: Evaluation of the Requirement for a Rapid Cyber Acquisition Process

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Butler, Matt J., Maj, USAF

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)
Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/ICW/ENG/12-03

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Force Institute of Technology, Center for Cyberspace Research
Attn: Dr. Harold J. Arata
2950 Hobson Way
WPAFB OH 45433-7765
(937) 255-3636x7105 (DSN: 785-3636x7105) harold.arata@afit.edu

10. SPONSOR/MONITOR'S ACRONYM(S)
AFIT/CCR

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES
This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

14. ABSTRACT

The Department of Defense has a standardized acquisition construct for delivering capabilities in the land, air, sea and space domains. Recently, cyberspace was identified as a warfighting domain; however, the unique attributes of the cyberspace domain require a more rapid process to deliver capabilities to the warfighter. Indeed, from initial requirements to fielding of the F/A-22 aircraft was approximately 20 years; this timeframe is not acceptable for cyberspace capabilities. To address requirements associated with the quickly evolving technology, senior leaders have called for a rapid cyber acquisition strategy. In response, methodologies have been proposed to enable quick response acquisition programs. On the surface, this notion appears viable. Examination, however, reveals that there has yet to be an Air Force program within the cyberspace domain that necessitates a rapid acquisition process. Rather, findings demonstrate that requirement for rapid delivery of cyberspace capabilities is more aptly associated with fielding tactics, techniques and procedures (TTP). This research examines the rapid delivery of cyberspace capabilities and challenges the paradigm associated with the need for rapid cyber acquisition. Results of the research demonstrate a need to shift focus from rapid acquisition to rapid TTP delivery.

15. SUBJECT TERMS
Cyberspace, Acquisitions, Tactics, Rapid, Capabilities, Requirements, TTP

16. SECURITY CLASSIFICATION OF: U			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Jonathan W. Butts, PhD (ENG)
a. REPORT U	**b. ABSTRACT** U	**c. THIS PAGE** U	UU	75	**19b. TELEPHONE NUMBER** *(Include area code)* (937)257-3636x4527; Jonathan.butts@afit.edu